DOCUMENT RESUME

ED 097 877 IR 001 238

AUTHOR	Renninger, Clark R., Ed.
TITLE	Approaches to Privacy and Security in Computer Systems. Publication No. 404.
INSTITUTION	National Bureau of Standards (DOC), Washington, D.C. Inst. for Computer Sciences and Technology.
REPORT NO	NBS-404
PUB DATE	Sep 74
NOTE	85p.; Proceedings of a Conference Held at the National Bureau of Standards, March 4-5, 1974
EDRS PRICE	MF-$0.75 HC-$4.20 PLUS POSTAGE
DESCRIPTORS	*Computer Programs; *Computers; Conference Reports; *Confidentiality; *Confidential Records; *Data Bases; Information Needs; Information Networks; Professional Associations; Public Policy

ABSTRACT

A conference was held at the National Bureau of Standards on March 4-5, 1974 to continue the dialogue in search of ways to protect confidential information in computer systems. Proposals were presented for meeting governmental needs in safeguarding individual privacy and data confidentiality that were identified at a conference held in November 1973. Among the proposals were the enactment of privacy legislation, improved computer system architecture and access controls, information and security management guidelines, and the development of a systematic, balanced approach to system security. The proposals were presented by legislators, citizens, computer industry associations and companies, professional societies, and public interest groups. (Author/WH)

ED 097877

BEST COPY AVAILABLE

Approaches To
PRIVACY and SECURITY in COMPUTER SYSTEMS

Proceedings of a Conference
Held at the
National Bureau of Standards
March 4-5, 1974

Clark R. Renninger, Editor

Institute for Computer Sciences and Technology
National Bureau of Standards
Washington, D.C. 20234

U.S. DEPARTMENT OF HEALTH
EDUCATION & WELFARE
NATIONAL INSTITUTE OF
EDUCATION
THIS DOCUMENT HAS BEEN REPRO-
DUCED EXACTLY AS RECEIVED FROM
THE PERSON OR ORGANIZATION ORIGIN-
ATING IT. POINTS OF VIEW OR OPINIONS
STATED DO NOT NECESSARILY REPRE-
SENT OFFICIAL NATIONAL INSTITUTE OF
EDUCATION POSITION OR POLICY

IR 001 238

U.S. DEPARTMENT OF COMMERCE, Frederick B. Dent, *Secretary*
NATIONAL BUREAU OF STANDARDS, Richard W. Roberts, *Director*

Issued September 1974

BEST AVAILABLE

National Bureau of Standards Special Publication 404

Nat. Bur. Stand. (U.S.), Spec. Publ. 404, 84 pages (Sept. 1974)

CODEN: XNBSAV

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 1974

For sale by the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402
(Order by SD Catalog No. C13.10:404). Price $1.20

NATIONAL BUREAU OF STANDARDS

The National Bureau of Standards[1] was established by an act of Congress March 3, 1901. The Bureau's overall goal is to strengthen and advance the Nation's science and technology and facilitate their effective application for public benefit. To this end, the Bureau conducts research and provides: (1) a basis for the Nation's physical measurement system, (2) scientific and technological services for industry and government, (3) a technical basis for equity in trade, and (4) technical services to promote public safety. The Bureau consists of the Institute for Basic Standards, the Institute for Materials Research, the Institute for Applied Technology, the Institute for Computer Sciences and Technology, and the Office for Information Programs.

THE INSTITUTE FOR BASIC STANDARDS provides the central basis within the United States of a complete and consistent system of physical measurement; coordinates that system with measurement systems of other nations, and furnishes essential services leading to accurate and uniform physical measurements throughout the Nation's scientific community, industry, and commerce. The Institute consists of a Center for Radiation Research, an Office of Measurement Services and the following divisions:

Applied Mathematics — Electricity — Mechanics — Heat — Optical Physics — Nuclear Sciences[2] — Applied Radiation[2] — Quantum Electronics[3] — Electromagnetics[3] — Time and Frequency[3] — Laboratory Astrophysics[3] — Cryogenics[3].

THE INSTITUTE FOR MATERIALS RESEARCH conducts materials research leading to improved methods of measurement, standards, and data on the properties of well-characterized materials needed by industry, commerce, educational institutions, and Government; provides advisory and research services to other Government agencies; and develops, produces, and distributes standard reference materials. The Institute consists of the Office of Standard Reference Materials and the following divisions:

Analytical Chemistry — Polymers — Metallurgy — Inorganic Materials — Reactor Radiation — Physical Chemistry.

THE INSTITUTE FOR APPLIED TECHNOLOGY provides technical services to promote the use of available technology and to facilitate technological innovation in industry and Government; cooperates with public and private organizations leading to the development of technological standards (including mandatory safety standards), codes and methods of test; and provides technical advice and services to Government agencies upon request. The Institute consists of a Center for Building Technology and the following divisions and offices:

Engineering and Product Standards — Weights and Measures — Invention and Innovation — Product Evaluation Technology — Electronic Technology — Technical Analysis — Measurement Engineering — Structures, Materials, and Life Safety[4] — Building Environment[4] — Technical Evaluation and Application[4] — Fire Technology.

THE INSTITUTE FOR COMPUTER SCIENCES AND TECHNOLOGY conducts research and provides technical services designed to aid Government agencies in improving cost effectiveness in the conduct of their programs through the selection, acquisition, and effective utilization of automatic data processing equipment; and serves as the principal focus within the executive branch for the development of Federal standards for automatic data processing equipment, techniques, and computer languages. The Institute consists of the following divisions:

Computer Services — Systems and Software — Computer Systems Engineering — Information Technology.

THE OFFICE FOR INFORMATION PROGRAMS promotes optimum dissemination and accessibility of scientific information generated within NBS and other agencies of the Federal Government; promotes the development of the National Standard Reference Data System and a system of information analysis centers dealing with the broader aspects of the National Measurement System, provides appropriate services to ensure that the NBS staff has optimum accessibility to the scientific information of the world. The Office consists of the following organizational units:

Office of Standard Reference Data — Office of Information Activities — Office of Technical Publications — Library — Office of International Relations.

---

[1] Headquarters and Laboratories at Gaithersburg, Maryland, unless otherwise noted; mailing address Washington, D.C. 20234.
[2] Part of the Center for Radiation Research.
[3] Located at Boulder, Colorado 80302.
[4] Part of the Center for Building Technology.

Foreword

This second conference on Privacy and Security in Computer Systems completes the initial step in what we hope will be a continuing process whereby all responsible and interested groups will work cooperatively in dealing with the complex issues of privacy and data confidentiality.

The National Bureau of Standards is grateful to all those who responded to this opportunity for identifying governmental needs for safeguarding personal and valuable information and suggesting approaches for meeting these needs. We are especially heartened by the broad spectrum of organizations who participated in these conferences: legislators, governmental agencies at the Federal, State and local levels, public interest groups, the computer industry, professional associations and societies, universities, trade associations, and individual citizens.

We believe this demonstration of interest on the part of so many persons and organizations indicates not only a deep concern for the problems of privacy and data confidentiality, but also the promise of accelerated attention to the development of sound legislative policies, administrative procedures and technological safeguards by which these problems can be resolved.

RUTH M. DAVIS
Director
Institute for Computer
Sciences & Technology

Abstract

This publication summarizes and contains the proceedings of a conference held at the National Bureau of Standards on March 4–5, 1974 to continue the dialog in search of ways to protect confidential information in computer systems.

Proposals are presented for meeting governmental needs in safeguarding individual privacy and data confidentiality that were identified at a conference held in November 1973. Among the proposals are the enactment of privacy legislation, improved computer system architecture and access controls, information and security management guidelines and the development of a systematic, balanced approach to system security.

The proposals were presented by legislators, citizens, computer industry associations and companies, professional societies, and public interest groups.

Key words: Computer systems; confidentiality; privacy; privacy and security; security.

Contents

	Page
Foreword	iii
Abstract of the Report	iv
Purpose of the Conference	vii
Summary of the Conference	vii
Conference presentations:	
INTRODUCTION	
Welcoming Address: Richard W. Roberts	1
Opening Address: Betsy Ancker-Johnson	1
LEGISLATION TO SAFEGUARD PRIVACY	
The Privacy Issue: Arthur R. Miller	2
Current Legislative Proposals in Congress: Edward I. Koch	3
Current Legislative Proposals in Congress: Barry M. Goldwater, Jr.	5
A Citizen's View of the Privacy Issue: Jane L. Hardaway	6
The Issues of Privacy and Computer Security Within the State of Ohio: Stanley J. Aronoff	8
The Issues of Privacy and Computer Security Within the State of California: Mike Cullen	10
The Issues of Privacy and Computer Security Within the State of Massachusetts: Arthur R. Miller	11
INDUSTRY VIEWS	
The Views of the Computer and Business Equipment Manufacturers Association (CBEMA): Peter F. McCloskey	16
A Call for Non-Proprietary Security Systems: August C. W. Biddle	19
The Views of the Association of Data Processing Service Organizations: John B. Christiansen	21
PROFESSIONAL ASSOCIATION VIEWS	
The Professional Aspects of Privacy and Confidentiality: Robert W. Rector	22
Data Processing Management Association Statement on Privacy and Security in Computer Systems: Donn W. Sanford	25
A SYSTEMATIC APPROACH TO DATA SECURITY	
A Systematic Approach to Data Security: R. L. Thomas and Robert H. Courtney	26
SECURITY IN COMPUTER NETWORKS	
Peter S. Browne	32
COMPUTER SYSTEM ARCHITECTURE AND ACCESS CONTROLS	
Oliver R. Smoot, Chairman of Panel	37
Security Architecture Using Encryption: Richard R. Keys and Eric H. Clamons	37
Access Controls in Burroughs Large Systems: Harvey W. Bingham	42
Systems Architecture for Security and Protection: James P. Anderson	45
Pragmatic Approaches to Software Security: Richard L. Caplan	50
INFORMATION AND SECURITY MANAGEMENT	
Joseph F. Cunningham, Chairman of Panel	53
Risk Analysis in Planning for Physical Security: Robert V. Jacobson	54

Page

Security Considerations in Information Systems Design:
Steven B. Lipner ---- 55
Auditing Current Systems: Donn B. Parker ---- 59

OPEN FORUM
The Medical Patient's Right to Privacy: Lois A. Bowden ---- 62
Confidentiality of the Medical Record: Margaret Beard ---- 63
Model Legislation: Brian Backus ---- 63
On Information Files and People: Mark P. Kriger ---- 64
The Need for Privacy Legislation: Robert H. Long ---- 65
The Administrative Burdens of Privacy Legislation: Edwin I. Golding ---- 66

CONFERENCE RESULTS
Ruth M. Davis ---- 67

Appendix A—Conference Program ---- 69

Appendix B—Executive Summary, Conference on Privacy and Security in Computer Systems, November 19–20, 1973 ---- 70

Purpose of the Conference

The second of two national conferences on Privacy and Security in Computer Systems was held at the National Bureau of Standards on March 4–5, 1974, to continue the dialog in search of ways to safeguard confidential information in automated systems.

The first conference, held in November, 1973, featured governmental spokesmen who described the needs and problems of Federal, state and local agencies in protecting confidential and valuable data from loss or misuse while at the same time providing free access to information concerning the public's business.[1]

The second conference provided the opportunity for persons or organizations to offer views and proposals on how these governmental issues might be resolved.

The conference was attended by 376 persons: 265 from government and 111 from the private sector. The attendees represented four congressional offices, 36 Federal agencies, 23 states, six municipalities, 33 computer companies or consulting organizations, three trade associations, and 20 professional associations, universities and public interest groups. Total registration at both conferences was 886. In his welcoming remarks, Dr. Richard W. Roberts, Director, National Bureau of Standards, observed that this broad spectrum of interest was demonstrative recognition that all groups must work together in harnessing the highly automated information systems that serve so many areas of our society.

Dr. Betsy Ancker-Johnson, Assistant Secretary for Science and Technology, Department of Commerce, noted that the President's February 23, 1974, statement on the American Right to Privacy accentuated the crucial nature of the privacy issue and the urgency of purpose represented by the conference objectives.

Summary of the Conference

Introduction

The privacy issue has come of age. According to Arthur R. Miller, Professor of Law at Harvard Law School, extensive legislative and judicial activities at all levels of government and the President's appointment of a Committee on the Right of Privacy make it clear that this problem of the intersection between the rights of people and the need to maximize the utility of a vibrant technology has now achieved legitimacy in our society. The time for action is at hand.

The clamor for action has come none too soon for Jane L. Hardaway, Commissioner, Department of Personnel, Tennessee. Speaking as an individual citizen, Mrs. Hardaway expressed her deep concerns over the trend toward increased fact gathering and the threats to personal privacy that may result from intentional or careless misuse of such information. Questions that urgently need answers, she said, are:

> "What power should the government have in fact gathering and what power should the government have to protect its citizens from other potential threats to personal privacy? What rights do the citizens have for protection against governmental abuses, and finally, what restraints of law should be applicable to all levels of government for the protection of those rights?"

Special pleas for the protection of the privacy rights of medical patients were made by Margaret C. Beard, American Medical Record Association, and Lois A. Bowden, American Hospital Association. In their view, increasing pressures for the release of medical information for educational, research, administrative and other needs require that legislation must assure the patient of the confidentiality of personal and sensitive information which he shares with health care professionals.

[1] An Executive Summary of the November 1973 Conference is attached as Appendix B. The complete report has been published under the title Government Looks at Privacy and Security in Computer Systems (NBS Technical Note 809). The publication may be ordered from the Superintendent of Documents, Washington, D.C. 20402 (Catalog C13.46:809), price 85 cents.

Legislative Proposals

The protective measures sought by a concerned citizenry are now being actively considered by the Congress with a growing sense of urgency.

"If there is any legislation," said Congressman Edward I. Koch (N.Y.), "that I believe requires the support of everyone . . . it's legislation to ensure the right of privacy." His specific proposals include H.R. 12206 and H.R. 12207 which provide for persons to be apprised of records concerning them which are maintained by government agencies; and H.R. 9786 which basically would apply the same provisions to all data banks identifiable to individuals.

Congressman Barry M. Goldwater, Jr. (Calif.) also urged congressional action, declaring that it is not enough to discuss the technology of the computer and speak of privacy in an abstract fashion. "We must resolve," he said, "to do what is necessary to protect our constitutional right to privacy." Specifically, he proposed consideration of his bill H.R. 11275 which sets forth a code of fair information practices, based on the report entitled, "Records, Computers and the Rights of Citizens," released in July 1973 by HEW's Advisory Committee on Automated Personal Data Systems. Other Goldwater proposals would limit the use of the Social Security Number, allow consumers to inspect credit records, protect individuals from statistical reporting systems and establish a select committee on privacy.

(Editor's note: Subsequent to the Conference, Congressmen Koch and Goldwater cosponsored a new bill, H.R. 14163 to define information practices to be followed with respect to personal data files maintained by both the government and the private sector.)

At the State level, legislative activity in the general field of data protection is also intensifying. Assemblyman Mike Cullen (California), noting that California voters responded to the issue of privacy in 1972 by amending the State constitution to declare privacy as an inalienable right of all persons, described several legislative and administrative measures already taken by the State to safeguard that right, including its current consideration of a proposal (Bill No. 2656) to establish a code of fair information practices. Professor Miller recited similar types of activities underway in Michigan, Minnesota, Massachusetts and numerous other States.

State Senator Stanley J. Aronoff (Ohio) took note of the proliferation of legislative activity across the country and suggested that the Code of Fair Information Practices bill which he introduced into the Ohio General Assembly should become the model for all privacy legislation in the 50 States. "Because of the ability of computers to talk to each other—city to city, State to State—," said Senator Aronoff, "I think it is important to develop as much uniform legislation as we can. That way, a person has a better chance to know and understand his rights no matter where he lives."

The need for uniform legislation to avoid the burden and confusion of a mass of conflicting requirements was a constant theme by speakers throughout the Conference. A specific proposal for addressing this problem was advanced by Brian Backus, representing the Government Management Information Sciences organization who called attention to a joint effort with the National Association of State Information Systems to develop model legislation for the consideration of all States.

Not everyone was convinced that legislative controls over personal data systems are necessary, however. Speaking during the Open Forum, Mr. Robert H. Long, Director of ACT, Bank Administration Institute, questioned whether there was sufficient evidence of privacy violations to warrant the registration and monitoring of automated personal data systems. "The way to protect privacy and confidentiality," he declared "is to improve the procedures of redress, not to attempt to control every personal data file at a governmental level." Dr. E. I. Golding, Office of Law Enforcement, Department of the Treasury, added the caution that before laws are enacted, indepth consideration should be given to coping with the administrative burdens that could result from carrying out the law. "They could be horrendous," Mr. Golding said.

In concluding the discussion of legislative proposals, Professor Miller noted that many of the proposals now appearing are technologically unsound, administratively unworkable, or placebos that offer the people no real protection. "The important single role for governmental policymakers," he said, "is to help the legislators find a mid-course between the extremes; otherwise, we will wind up with bad legislation."

Industry Implications

Striking a proper balance between the protection of personal privacy and the provision of efficient government services was a concern also expressed by computer industry spokesmen. Peter F. McCloskey, President, Computer and Business Equipment Manufacturer's Association, offered the suggestion that satisfactory resolution of the issue must be approached from a systems viewpoint in which the separable issues of privacy, confidentiality and data security are addressed in interrelated fashion. He said that the prolifieration of diverse legislative proposals "dramatically points up the need for a clear understanding of the benefits versus the cost trade-offs to be obtained."

Unfortunately, according to John Christiansen, speaking for the Association of Data Processing Service Organizations (ADAPSO), the bills proposed to date for accomplishing the commendable goal of safeguarding personal information "demonstrate an ignorance of the specific economic characteristics and problems of the computer industry. Especially, the potential costs of compliance could be disastrous for the small, independent data processing service companies. ADAPSO urges an intensified effort to provide greater knowledge of the issues, costs and consequences before embarking on legislation or regulation."

The Computer Industry Association is concerned that the technological development of secure data processing systems represents a complex, expensive and time consuming undertaking that exceeds the human and financial resources available to all but the largest of the manufacturers. Further, A. G. W. Biddle, Executive Director of the Association, believes that the independent development of security technology by only one or a few of such suppliers would be detrimental to the user, the public and the industry as a whole. To avoid these consequences, Mr. Biddle suggested that serious consideration should be given to the creation of a federally chartered nonprofit "Super Underwriters Laboratory," charged with the responsibility for developing and disseminating technological solutions to the data security problem. In pursuing this approach, said Mr. Biddle, "We will increase the likelihood that secure systems can be available on a timely and economic basis. It certainly represents an improvement over a dozen noncompatible proprietary solutions."

Contributions of Professional Societies

No technological advance is effective without a sense of professional responsibility among the people involved. Thus, there is a compelling need, said Robert W. Rector, Executive Director of the American Federation of Information Processing Societies, for the computer professional to exert his influence upon solving the problems of privacy and security. According to Mr. Rector, the principal motivation for the professional societies' interest in privacy is protection of the general public welfare and its function of promoting professional objectives through education.

Examples of the societies' educational activities were cited by Joseph F. Cunningham, Executive Director, Association for Computing Machinery. The ACM has cooperated with the National Bureau of Standards in sponsoring a workshop on the technical aspects of controlling access to computer systems and in planning for the provision of guidance on procedures for data security in selected public services.

Donn W. Sanford, Executive Director, Data Processing Management Association, warned against hastily developed privacy procedures or laws which could be as onerous as the ills they seek to rectify. Expressing full DPMA support of a positive, balanced and realistic approach to the privacy issue, Mr. Sanford revealed that a newly drafted "Standards of Ethical Professional Practice Regarding Individuals' Rights of Privacy" is under consideration for early adoption.

Computer System Architecture and Access Controls

While solutions for safeguarding the privacy of individuals are to be found in legislative or regulatory proposals, solutions for protecting confidential data in automated systems are found in technological safeguards and procedures through which access to the systems may be controlled.

The major computer architecture approaches to providing these safeguards, according to James P. Anderson of the James P. Anderson Company, are based on the fundamental principle of isolation; i.e., providing mechanisms for isolating data that cannot be bypassed by the users of the system. These approaches include:

- virtual machines systems: creating an isolated environment through techniques which have the effect of creating for each user a complete system dedicated solely to his purposes. This approach is perhaps most applicable in service center operations where hardware resources are shared among different organizations, each with a need to protect their information from others.
- descriptor-based systems: creating an isolated environment through techniques which provide the authorized user with unbounded memory space unaccessible to others. This approach is most applicable in on-line time sharing or "utility" systems where there is a major requirement for sharing programs or data.

Both of the above approaches must be augmented with mechanisms for identifying users and authorizing their access to the system.

The architecture of current Burroughs large-scale systems anticipated the requirement for safe sharing of resources among users and provides many access controls to resist penetration. Harvey Bingham, Burroughs Corporation, said that software language barriers provides cross checks against errors. These controls may be further specialized to meet particular user needs.

Achieving security in computer networks is a greater challenge than achieving it in stand-alone systems. Even so, according to Peter S. Browne, General Electric Company, an adequate level of security in networks is possible with today's technology. The necessary conditions are minimum standards for physical protection, operational procedures, and audit. True network security, however, can only be achieved through modifications to systems software/hardware which, Mr. Browne explained, are not available in today's commercial systems.

A crucial issue in networking, as seen by Mr. Browne, is the capability to encrypt (code) data for transmission, a subject addressed more specifically by Richard R. Keys, Honeywell. In Mr. Keys' view, data encryption can increase the protection of data when used as part of a secure environment, but the technique by itself is not sufficient to protect a system. Better, faster encryption techniques and speedier, less costlier circuits are needed. Fortunately, Mr. Keys said, we are by no means at the end of our technological capability; but since encryption technology is a specialty of governments, the ultimate success of security architecture using encryption will depend on the willingness of the appropriate government agencies to help develop the algorithms needed to satisfy the design criteria of data processing machines.

Secure software also plays an essential role in data security which is too often overlooked. Using case examples, Richard L. Caplan, Advanced Computer Techniques Corporation, showed how, by focusing attention on improvements in the testing of user-created programs as well as the structuring and control of technical documentation, significant improvements in computer system security can be achieved.

A Systematic Approach to Data Security

In a joint presentation, R. L. Thomas and Robert H. Courtney, IBM Corporation, suggested that an effective security system must include the total environment: physical and procedural safeguards as well as those provided by hardware and software. Otherwise, unnecessary layering of security measures and high costs will result. The selection of those measures which, in balanced combination, provide the desired security at least cost should be determined by a systematic analysis of the reasons why there is concern for the safety of data (e.g., human errors, dishonest employees, fire) and upon an assessment of the probabilities of such occurrences and the consequences that will result.

Mr. Courtney focused his discussion on the merits and problems of security measures in four classifications: identification, authorization, audit and system integrity. Addressing the question of general guidelines for the design of hardware to eliminate potential data security problems, Mr. Courtney said that such guidelines can never replace continuous detailed review of the design of each specific product for potential problems, because it is impossible to conceive in advance all of the problems that might occur.

Although the demand for data security is growing, Mr. Thomas noted that customers still rank computer security features below other considerations, such as price, performance and other special capabilities. "It is our feeling," he said, "that the awareness and identification of the needs of security will increase in the future. And although certain tools and techniques are available today, we feel it would be wrong for the industry to wait until that demand becomes pressing before taking the necessary steps to meet the problem."

Information and Security Management Guidelines

The handling of security in a computer-based information system is at best a difficult problem. But deferring consideration of security issues has never been shown to be a viable way of handling the problem. Steven B. Lipner, the Mitre Corporation, suggested that the designer is best served by addressing security as he designs the system, building security measures into his design, and attempting to eliminate those problems he cannot solve. In designing an information system that handles sensitive information, he said, assessments of threat and vulnerability are basic.

Mark Kriger, Harvard University, cautioned that system designers must also be wary of the "information flashpoint" at which separately maintained nonconfidential data may suddenly become confidential when merged.

In making assessments of threats and vulnerabilities, reliance on ritual is too often substituted for rational thought. Robert V. Jacobson, the Sentor Security Group, Inc., suggested that the first step in a rational approach is to define computer system security as:

- protection against losses caused by delays in completing assigned data processing tasks
- protection of assets against loss, theft or misuse

By analyzing security needs on this basis, it can be clearly seen which are the most significant threats and which have the greatest potential for loss. From this information, security measures can be focused on areas of greatest need, a reasonable level of security expenditures can be determined and a foundation for security audit can be formed.

The security audit function thus is viewed as an integral part of the security management process. It provides a review of the adequacy and effectiveness of the security measures that have been put in place and points toward improvements that are needed. Current auditing methods, however, generally reflect a lack of awareness of the vulnerabilities associated with computers, explained Donn B. Parker, Stanford Research Institute, because newer technologies are causing basic changes in the operational methods, the occupations of people and the scope of the functional activity to be protected. To solve this problem, he said, it is necessary to develop and document good practices for auditors which match the advancement of systems they must audit.

Next Steps

This Conference and the initial Conference held in November 1973 will have served their purpose if they lead to action-oriented programs which can ease the problems of data confidentiality and computer security. Noting the wide spectrum of actions proposed by the Conference participants, Dr. Ruth M. Davis, Director, Institute for Computer Sciences and Technology, National Bureau of Standards, summarized these as follows:

- enact cohesive privacy legislation at the national and State levels of government which gives proper consideration to the administrative, technological and cost impacts of compliance.
- develop and apply an effective balance of managerial, administrative and technological measures in safeguarding data confidentiality.
- enlarge the educational activities needed to improve understanding of the privacy, data confidentiality and computer security issues.
- stimulate research and development of technological safeguards in the private sector by providing legislative policies, standards and security requirements.
- determine costs of data confidentiality as a basis for decision and allocation among those who must bear the expense.

Implied by these broad categories of action are numerous activities for which no single group or organization in either the public or private sector has total responsibility. Progress will depend upon the initiatives taken by all those who bear specific responsibilities or can contribute uniquely to achieving privacy and data confidentiality—the Congress and State legislatures, government agencies, program managers, computer and related industries, professional and trade associations, and public interest organizations.

The Conferences have confirmed the complexity of the problem and the difficulties in providing solutions. But, said Dr. Davis, "I think, happily, we're now entering the productive stage. We're now talking rationally and reasonably. We have heard people give very thoughtful and deliberate approaches to the problem. We're going to make every attempt to get the views expressed here to all of those people to help them carry out their responsibilities."

WELCOMING ADDRESS

Richard W. Roberts
Director, National Bureau of Standards
Washington, D.C. 20234

I am pleased to welcome all of you to this second conference on privacy and computer security. Our purpose here is to continue the dialogue we started in November in search of ways to preserve the privacy of individuals. This task is many-sided. Today and tomorrow we will consider ways of harnessing the highly automated information systems that serve so many areas of our society.

In order for that assessment to be meaningful, people at all levels must work together. In this way the products of research, present and future, can yield the maximum benefit.

By participating in this conference, you show that you recognize the need for coordinated effort. The essential link between legislative and technological safeguards is attested to by the presence this morning of two members of Congress and two State legislators: Congressman Edward Koch; Congressman Barry Goldwater, Jr.; State Senator Stanley Aronoff; and Assemblyman Mike Cullen. Each is actively sponsoring an important legislative proposal in the field of privacy, and they have come to share their time and views with us.

Two people known for their concern with the privacy of individuals, Professor Arthur Miller of Harvard, and Mrs. Jane L. Hardaway have consented to provide commentary on these and other legislative needs and activities.

People responsible for implementing data confidentiality requirements are also represented. The Computer and Business Equipment Manufacturers Association, the Computer Industry Association, and the Association of Data Processing Service Organizations are with us, as are numerous computer companies and consulting organizations.

Professional societies have always been regarded as a valuable source of assistance in national problems having a strong technical orientation. Members of the American Federation for Information Processing Societies, the Data Processing Management Association, and the Association for Computing Machinery have come to offer their insights.

We believe that the diversity of views presented during these next two days can make this conference useful and productive. We at NBS are happy to be your hosts and are pleased to make our facilities available for your meeting. I know that those responsible for this conference, in particular Dr. Davis and Mr. Renninger, will try their best to make your visit a pleasant one.

And now I would like to present to you the Honorable Betsy Ancker-Johnson, Assistant Secretary of Commerce for Science and Technology.

OPENING ADDRESS

Honorable Betsy Ancker-Johnson
Assistant Secretary for Science and Technology
Department of Commerce, Washington, D.C. 20230

On behalf of the Department of Commerce, I am especially pleased to greet you. We welcome your participation in this effort to help resolve the issues of privacy and security in computer systems, and we are happy to provide resources for your work. I know it is a great pleasure for Dr. Richard W. Roberts, Director of our National Bureau of Standards, to host this second conference on privacy and security in computer systems.

Our first conference in this continuing series identified major issues related to free access to information in connection with the public's business.

The primary governmental concerns identified at the November conference were:

First, achieving national coherence among laws defining both individual rights of privacy and the basic information practices to be followed in protecting these rights;

Second, applying existing technology to enhance computer security in present systems;

Third, insuring that the necessary new technology is developed to satisfy growing security needs;

Fourth, establishing uniform management and technical procedures for effecting security measures;

And, finally, developing and implementing a mechanism for allocating the costs of computer security among public, industrial, and government sectors.

We are here at this second conference to learn your proposals for resolving any conflict between full application of computer technology and the protection of personal privacy. Personal privacy is one of our most valuable yet vulnerable rights. As Americans from the Pilgrims on, we demand the right to control the collection of personal information about ourselves. In fact, the Pilgrims were essentially seeking privacy by coming to America in the first place. One utterly con-

sistent, enduring characteristic of the people comprising what an earlier generation described as a "melting pot"—whether these people be native Americans, descendants of the Pilgrims, or more recent arrivals from whatever corner of the world—is our insistence on controlling the use of personal information about ourselves.

We know that information concerning over 150 million Americans is now in computer banks scattered across the country. "Until the day comes when science finds a way of installing a conscience in every computer, we must develop human, personal safeguards that prevent computers from becoming huge, mechanical, impersonal robots that deprive us of our essential liberties," as President Nixon said in his address on the American Right of Privacy, February 23rd.

We in the Department of Commerce have been dealing with computer technology issues since the middle of the century. It was then that the National Bureau of Standards built one of the first electronic computers, SEAC (the Standards Eastern Automatic Computer). Our computer programs at NBS are charged with three major responsibilities:

First, developing mandatory Federal automatic data processing standards;

Second, providing consulting services in the computer field for Federal agencies, and

Third, undertaking research in computer science and technology.

Several years ago the Department, recognizing the critical importance of computer security, formed a special computer security program as a priority component of its Institute for Computer Science and Technology (ICST).

President Nixon's recent statement stressed the crucial nature of this issue and his formation of a special Domestic Council committee on the right of privacy greatly emphasized the important work that Dr. Ruth Davis, Director of ICST, has already well underway. The President has charged the committee with recommending "direct, enforceable measures" which can be put into immediate effect to provide a personal shield for every American's sense of privacy. These recommendations are due within four months, let us all note. Secretary of Commerce Frederick Dent, who is pleased to be one of the ten members on this committee, will be especially well prepared to contribute because he has all of you helping him.

And so we see that our conference issues have been accorded the highest level stature and priority. Our urgency of purpose in gathering today and tomorrow to seek viable computer security measures couldn't be greater.

Both Secretary Dent and I are committed to the goals of this conference. We are eager to hear and work on your output.

THE PRIVACY ISSUE

Arthur R. Miller
Harvard Law School, Cambridge, Massachusetts 02138

A special word of thanks for the hospitality of the Department of Commerce in sponsoring this second conference. Those of us who have been working in the privacy field since the proposal for the national data center emerged in 1966 and 1967 realize what a tremendous maturation process has occurred in the six years since that time. In those days the issue of computers and privacy was a highly emotional issue. The metaphors of those days were "Womb to Tomb" dossiers, "1984," "computer infallibility," society becoming a glass house. From the computer enthusiasts on the other side of the dispute, we kept hearing such things as social planning, solving the problems of a complex society, the need to apply technology to man's needs, and, fear not, we are only using it for socially desirable purposes.

Because of the emotional tone of that debate, more heat was generated than light. I feel perfectly comfortable in saying that because during that period I was one of the heat generators. Fortunately, in the six years we have learned a great deal about the issue, the stakes that are involved, the need of the technical community to be in touch with the legal, civil liberties, and consuming communities, to develop a better feel for the legitimate and the illegitimate applications of technology and social planning based on personal information.

So it is with joy that in early 1974 we can announce that the privacy issue has come of age. The events of the last year as well as the proposals put forward during the last year all make it clear that this problem of the intersection between the rights of people and the need to maximize the utility of a vibrant technology has achieved a legitimacy in our society that was undreamed of in 1967 when two sides stood across the river and threw rocks at each other. In the past year we have had the publication of the Department of Health, Education, and Welfare's report on Automated Personal Data Systems, a report which I personally believe (and obviously I am biased because of having served on the committee) is probably one of the most advanced and most sensitive statements of the problem and of possible solutions. Since the publication of the HEW report, we have had a flurry of legislative activity. There have been legislative proposals, such as those we will hear more about this morning by Congressman Koch and Congressman Goldwater, presenting to the Congress two basic models for regulating technology to achieve the much needed balance between technology and privacy. We have, as Dr. Ancker-

Johnson just indicated, the President giving personal attention to the privacy issue. He has done this through a very clear statement in the 1976 State of the Union Message and in last Saturday's statement on privacy and the appointment of a committee on privacy at the cabinet level with a mandate to report in four months. This short-term mandate seems to me to reflect the fact that the time for rock throwing is over, the time for study is over (we have more studies than we probably need), and the time for action is at hand.

At the State level, we not only have legislation activity, we have legislative fruition. In the field of arrest records, Alaska, Iowa and Massachusetts have enacted comprehensive data protection statutes dealing with criminal justice information. Comparable legislation is now pending in upwards of fifteen other States. In the general field of data protection, we have legislative activity comparable to the efforts of Congressmen Koch and Goldwater in Michigan, California, Ohio, Massachusetts, Minnesota, and probably five or ten other States that have not come to my attention with a good prospect of legislative action in some of these States this year.

The courts have seen an increased number of actions brought by public interest organizations, social activists, the ACLU, concerned citizens, and consumer groups, trying to challenge and rectify some of the imbalances in our traditional legal approach to matters of privacy. The issue even has achieved international dimensions. Sweden has enacted a comprehensive data base protection act. The Federal Republic of Germany may legislate on the subject this year. The Japanese, the English, the Danish, the French, and the Italians all are contemplating legislative proposals. OECD, through its Computer Utilization Group and its Data Bank panel is now engaged in extensive study and the formulation of recommendations with regard to the multinational use of personal information.

Finally, the United States Supreme Court a year or so ago decided Roe versus Wade which some of you will recognize as the abortion decision. Most people think it is simply an abortion case. If you read it carefully, it also is a privacy case. For the first time in American legal history we have a clear and unequivocal statement by the Supreme Court that there is a constitutional right of privacy in this country that cannot be undermined by the State. In the Roe case, the intrusion took the form of an attempt by a State to outlaw abortion. It is perfectly clear, of course, that conservative readers of the case will say that to the extent it recognizes a constitutional right of privacy, Roe can be limited to a right of privacy relating to the human body. Even that is not an unqualified right because no one would say we have a constitution right to commit suicide, which arguably involved privacy of the body. A liberal reading of the opinion, however, would be that although this case happened to involve an abortion or physical or body privacy that does not mean that the Roe case cannot be applied beyond that context and extended to spatial privacy, or associational privacy, which in effect already has been recognized in earlier cases and, most important of all from our perspective, information privacy. We are just going to have to wait and see how subsequent cases interpret and apply Roe.

Thus, it is quite appropriate that we are conducting this panel this morning on legislative proposals in an attempt to explore some of the details and the direction these legislative and administrative proposals are taking. They are numerous but they follow relatively well defined formats and hopefully during the next three hours the members of the panel will be able to transmit some sense of what is going on in the Congress, the State legislatures and the regulatory bodies. The expectation, of course, is that somehow through this discussion of these activities you will come away with a sense of where the law is moving with regard to the computer security and computer privacy issue.

CURRENT LEGISLATIVE PROPOSALS IN CONGRESS

Congressman Edward I. Koch
House of Representatives, Washington, D.C. 20515

I was delighted at the invitation to participate in this Conference and am especially pleased to have the opportunity today to discuss my privacy legislation with you. I've been involved with the privacy issue since coming to Congress in January of 1969; and as Dr. Miller points out, we have come a long way—a very long way. I introduced the first privacy bill in the Congress on February 19, 1969, and to indicate how quickly Congress moves on this, it was not until exactly five years later on February 19, 1974, that hearings were held on the bill. This was an important breakthrough, however, because it showed, as Dr. Miller pointed out, the change in the climate.

Since this is not a lay audience that has to be converted, I will merely highlight the keypoints of the bill today. You're as familiar with the background as I am—indeed, more so, because of the technical aspects which you handle everyday. My bill contains the following provisions: It would open the files. It would permit every individual to see his or her own file, subject to some very reasonable safeguards. It would permit you to correct the files. It would permit you to add supplementary information which would explain material contained in the file that may be correct but which requires an explanation. It would limit what could be collected. Now, you would think that would

be something that the Administration could support. The witness who appeared before the Committee from the Justice Department—a very sympathetic, very good witness said, "Well, really, the Administration is not desirous of supporting this approach which attacks all of the agencies in this way. We want an agency-by-agency bill." That will take, not five years, that will take fifty years. And I think it is a delaying tactic. In my judgement, H.R. 12206 and H.R. 12207, both of which I authored, are more effective proposals. In deference to the Committee, I removed the Federal Privacy Board, which I think is important, from my original legislation; and H.R. 12206 permits each agency to provide its regulation separately. Each agency would publish its regulations, thereby permitting the flexibility that the Administration desires. I made this revision because there's a split on the Government Operations Committee with respect to any new boards—many members are opposed to establishing new boards. I happen to believe the Federal Privacy Board is very important, but in order to get the legislation through, I am willing to support the bill without the Federal Privacy Board and permit each agency to promulgate its own regulations. As people begin to gain access to their files, it is my hope that ultimately a board or some intergovernmental agency would assume those functions, however, in a comparable manner to the Freedom of Information Act. That's bill number one.

Bill number two is the more comprehensive bill, H.R. 9786, which is before the Judiciary Committee, and which would regulate all data banks whether government operated or privately operated. As you know, H.R. 12206 covers government data banks; H.R. 9786 covers all data banks but contains basically the same provisions as H.R. 12206 plus the Federal Privacy Board.

Let me share with you a couple of experiences indicating why it's necessary that we do something here. As a result of a press release issued by Acting FBI Director L. Patrick Gray, I learned in October 1972 that the FBI was discontinuing the practice of collecting dossiers on members of Congress. So I wrote him a letter. I said, "Terrific, please send over my dossier." He wrote back, saying, "No. (I had misunderstood) that the FBI was not collecting dossiers. It was simply collecting newspaper clippings and biographical material." So I said, "Send over my clippings and my biographical material." He responded to the effect that, "We only do that on a need-to-know-basis and you don't need to know." As you know, he was not confirmed and his successor was William Ruckelshaus. I sent the same correspondence, got the same response, and he was not confirmed. The third and current Director is Clarence Kelly. When he was confirmed, I sent him a note: "Dear Director, I hope there's a change. I'd like my file." He responds, "We don't have a file on you." I write back, "That's strange in view of the prior correspondence. Won't you look again?" He writes back, "How many times do I have to tell you, we don't have a file on you. We do have your name in a cross index to find your voluminous correspondence. If you think we should not, feel free to introduce legislation." I write back, "Terrific letter, great sense of humor, let's have lunch."

I called him and although we couldn't have lunch, he came to my office with his assistant. First thing I said was, "Mr. Director, you said you don't have a file on me and I accept that. But you do have files on other members of Congress." His assistant says, "Just a minute, Congressman. We want to make something very clear. The Director said we don't have a file on you. We do have some memoranda, so that when we come over we'll have an opportunity to discuss with you matters which may be of interest to you and have some information about your interests." So, he said, "For example, we know you graduated from Fordham University." I said, "I didn't go to Fordham University. I went to CCNY."

Shortly after that meeting, I sued the FBI to get my file. Finally, as a result of the change of the Attorney General, the agency agreed to furnish me with the material required under the Freedom of Information Act. And so the FBI sent over my alleged file. Now, what did it include? Well, it included my newspaper clippings. It included a flyer listing me in opposition to the A.B.M. It included my testimony before the Senate Committee on opposition to the confirmation of Acting Director Gray, and it also had a face sheet which I assume exists in every file. I'm going to read the face sheet to you.

It's official—"November 7, 1968, U.S. Government Memorandum. On November 5, 1968, Democrat Edwin I. Koch of New York City was elected to the 17th Congressional District held by retiring Representative Ted Kupferman. Koch was born in 24 in New York City." It goes on—he's a former councilman, he's been a Democratic leader since 1968. Then it says "information in Bu files." I assume that means Bureau files. "A check of Bureau indices reflects no reference identifiable with Koch." My reaction was that maybe if they had looked under my real name, not Edwin Koch, but Edward Koch, they would have come up with my file.

Now, I mention this to you to indicate the need for legislation in this area. Now, the errors, if you will, the irrelevancies relating to me and to my files, are not of any great moment; but if we make those errors, how many other errors are there that will never be found and that will remain in the files of individuals, constantly affecting their progression either in government or outside of government. So, if there is any legislation that I believe requires the support of everyone, conservatives and liberals alike, it's legislation to ensure the right of privacy. Thank you very much.

CURRENT LEGISLATIVE PROPOSALS IN CONGRESS

Congressman Barry M. Goldwater, Jr.
House of Representatives, Washington, D.C. 20515

Distinguished former colleague of mine, Congressman Jackson Betts, who was one of the pathfinders in promoting legislation to protect privacy, once said: "Privacy is not simply an absence of information about us in the minds of others; rather, it is the control we have over information about ourselves."

I am pleased to be a Congressional participant in the Conference sponsored by the Institute for Computer Sciences and Technology, here today.

Since coming to Congress almost five years ago, I have become increasingly concerned about the growing menace privacy invasion poses to the American citizen.

Early last year, I decided to initiate certain proposals to assure the American citizen that he would indeed have control, as mentioned by Congressman Betts, over information compiled and retained about him.

An initial report was to work very closely with the Secretary of Health, Education, and Welfare prior and after the release of the very extensive HEW study entitled "Records, Computers, and the Rights of Citizens." This report was released last July.

I was most impressed with this study, and in order to carry out its specific recommendations, I introduced two bills.

One, "The Freedom of Information Act," H.R. 11275, is basically aimed at accomplishing the following three objectives:

(1) To guarantee individuals the right to find out what information is being maintained about them in computerized systems and be able to obtain a copy of it upon demand.

(2) To allow a person to contest the accuracy, pertinence, and timeliness of any information in a computer-accessible record about him.

(3) To require record-keeping organizations to inform individuals on request of all uses made of information being kept about them in computerized files.

Shortly after introducing this bill, I joined with Massachusetts Governor Frances Sargent, Senator Edward Brooke, and Congressman Michael Harrington, in an administrative petition with the Justice Department, which asked former Attorney General Elliot Richardson to terminate operation of the F.B.I. Administered Offender Files, which are a part of the National Crime Information Center, until he had issued formal regulations to safeguard the rights of individual citizens.

Additionally, I introduced a bill to amend the Social Security Act, that would give each individual in this country the right to refuse to disclose his or her Social Security Number. Then too, organizations with the authority to use the number would be prohibited from disclosing the number to organizations that lack such authority.

This legislation is designed to prevent the Social Security Number from becoming a "Standard Universal Identifier" that can be used by computers to track all the errors, omissions, and/or sins of an individual from cradle to grave.

Other actions included the introduction of legislation to require consumer reporting agencies to allow a consumer to inspect credit records, legislation to protect individuals from statistical reporting systems, and a Bill to establish a select committee on Privacy in the House of Representatives. Recent events indicate that more and more people are becoming concerned about privacy invasion. This is a good sign, because I have always maintained that the worst enemy of privacy is not the computer—its worst enemy is apathy and ignorance.

I am pleased that the President addressed himself to privacy in his recent State of the Union Address. Just a few days ago, he announced the formation of a commission on the issue of Privacy and Data Banks in our country.

Suffice to say, it does us little good to attack the computer—it is only an instrument of man. What must be attacked is the computer mentality—the kind of faceless bureaucracy in and out of Government that seeks to make the computer a supreme being.

The potential of privacy invasion is always present in a sophisticated computer operation. Remarkably, the misuse of information held about individuals in computer systems has been held to a minimum. But the potential for misuse is still there, and certainly data surveillance has grown to very menacing proportions due to the technological advances which alter such information Given multiple use and consolidation through automated systems.

Substantial increases in demand for personal reports by Government Agencies, Private Systems, and Social Science Researchers have intensified the severity of the problem.

As you know, it is not enough for us to discuss the technology of the computer and speak of privacy in an abstract fashion. We must resolve, at this Conference, and in every other private and public forum to do what is necessary to protect our constitutional right to privacy.

Let us make no mistake about it, the computer already knows more about most of us than we know about ourselves. The amount of data held in computer systems is enormous. Think about it for a moment. The list includes tax returns, census responses, social security data, military records, security files, finger prints, FHA and VA mortgage guarantees,

credit records, health data, and social research involving individuals. Such examples are barely the tip of the iceberg.

I say tip of the iceberg because everytime Congress passes legislation giving the Federal Government added responsibilities and power, more paperwork is created and consequently more information is known about the individual citizen.

Of course, this is a sobering thought, but what can we do about it?

Initially, we must understand our right to privacy and how important it is to protect this right. Secondly, we must rely on wise laws that protect our privacy rights.

We must remember that our citizens give the Government personal information on what should be on a confidential basis and for a specific purpose. Americans deserve the assurance that this information will not be used for any other purpose in the future. But, do we have this assurance? Not necessarily, I fear.

Several years ago a House Congressional Committee discovered that the confidentiality of Government files is a myth. Such files sometimes float from agency to agency. Federal investigators in some instances are given access to information far removed from the subject of their inquiry. Folders sit open for inspection on desks and in the "in" and "out" baskets of many Government offices. Outright "leaks" of information occasionally come to light.

Of course this is interesting, you say. But, then you add that the Government has never misused the information about you, so why worry? But, I submit that this may not be the case in the future unless we begin to embark on a course to make certain that it will not be misused.

It is always possible for unscrupulous men in high places to apply unethical standards to the use of confidential information. One of History's leading examples is the detailed European census that was in effect long before the advent of Hitler. Tragically, this census provided a convenient and efficient tool for Nazi use in many European nations. In some countries like Czechoslovakia, statistical data already available facilitated the Nazi takeover.

Impossible here? Not necessarily. Erroneous data or information, whether computer-stored or not, can lead to bizarre occurrences that constiute a blatant invasion of privacy.

Two years ago 15 men wearing beards and dirty clothes took a battering ram and knocked down the door of a suspected violator of a Federal Gun Law. Did this happen in Soviet Russia? No, it happened near Washington, D.C. The suspect was a law-abiding citizen, who only collected harmless antique weapons. He is now totally paralyzed—his life is in shambles. The ruffians who perpetrated this crime? They were officials of the U.S. Treasury Department, and they broke into the victim's home on faulty information that he was in violation of the 1968 Gun Control Act.

This is not a remote example. Earlier this year, the same thing happened to a family in Winthrop, Massachusetts. A couple and their daughter, who was ill, were awakened in the middle of the night when State and Federal Lawmen broke down two doors to their home on a narcotics raid. The policemen had entered the wrong home.

Of course these are clear-cut examples of privacy invasion. There should be no question that they also violated the Fourth Amendment to the Constituion.

But, there are other examples almost as sinister in nature. I have received numerous letters from American citizens describing examples of Data Bank and Social Security number abuse. Each letter seems to detail a new horror story worse than the one before. Some of the letters have actually come from computer systems analysts in the field of data processing.

The protection of personal files in all data systems deserves immediate attention on the part of both the Government and the private sector. I would like to challenge this Conference to not only exchange ideas and make recommendations to assure the privacy of individual data subjects in computer operations, but I would like to see a definitive statement emanate from this Conference calling for a restoration of freedom of privacy.

It is not difficult to determine the adverse potential of today's technology on our right to privacy. What is difficult is making certain our traditional liberties and beliefs can be secure against growing technological onslaughts against privacy.

A CITIZEN'S VIEW OF THE PRIVACY ISSUE

Jane L. Hardaway
State of Tennessee Department of Personnel, Nashville, Tennessee 37219

I am most appreciative of the opportunity to be with you today to discuss the very important subject of the role of Government and the individual's right of Privacy. I find it altogether fitting and appropriate that this topic should be discussed by us in this place—Washington, the Nation's Capitol, for it is here that each citizen must still look to find not only properly exercised governmental authority but also legislative protection from improperly exercised authority.

The topic today vitally concerns our individual liberties. More than that, it concerns this Nation's ability to preserve such rights and still maintain the fabric of Government as it was intended by all of those who have, over the years, so hotly debated the subjects of liberty in this very city.

Constitutionally protected privacy of individual citizens in their persons, houses, papers and effects is not a new concept. It is as old as the Constitution itself.

In recent times, however, it has grown to hold more and more importance and be more constantly in the public eye. No one can long dispute the fact that our Government can and must exercise sufficient power over individuals both in and out of the country to protect itself from invasion or revolution. If this were not so, we should have long ago ceased to operate under our Constitution. When, however, does the exercise of such power cease to be proper and begin to encroach upon the rights of citizens?

During the decade of the sixties and early seventies, there was much unrest and violent dissent across the nation. I, like the vast majority of our citizens, was shocked and eventually enraged by the actions taken by those individuals and organizations whose primary purpose was the disruption and eventual overthrow of our governmental system. It was clear to me that in the name of a "better way," they felt that their ends justified any violent means, a philosophy too horrible for me to contemplate.

In my mind, the conviction held that it is not the Government's right but its duty to protect us and itself from such factions. Excesses resulting in such violence cannot be tolerated.

The Government did take action, indeed we have now learned that a great deal of activity has been taking place in the use of secret surveillance and personal data collections. In viewing what we now know to be the Government's actions in this regard, something has occurred to me. The Government, too, has been more than capable of excesses of power in the promotion of its interests. A Government of such power and size that it is considered the strongest on earth; a Government with such technical expertise at its disposal as to be almost science fictional in nature. This Government, with all of its power, expertise and knowhow, has been absolutely capable of overstepping constitutional powers and this, not against foreign elements threatening invasion, but against a small group of "so-called" citizens intent on the overthrow of our national framework but against us all. For in the final analysis, each of us, no matter how law-abiding, is threatened when Government violates its own legal precepts, no matter what theory is used to justify such acts. And it is my belief that such acts of power once abused will grow in abuse as the power grows to be utilized for it, unless there is restraint by law.

The questions then are posed anew: what power should the Government have in fact gathering and what power should the Government have to protect its citizens from other potential threats to personal privacy? What rights do the citizens have for protection against governmental abuses, and finally, what restraints of law should be applicable to all levels of Government for the protection of those rights? For these answers, we cannot look exclusively to history. We cannot look to actions taken by prior presidents, prior attorneys general or the prior actions of governmental agencies, for we now know that many times such actions were exercises of abuse. It is a new day and the answers to the new day's problems most certainly will be answered in the context of the future, not the past. Let me briefly discuss with you one area with much potential for danger for us all. Fact gathering, as I have stated earlier, in many ways can threaten the rights of citizens. I hope you will be able to see, as I have, that governmental action in derogation of our rights can be a monster of two heads and perhaps more. One head surely is illegal and unwarranted surveillance of citizens, the other is indiscriminant and abusive personal data collection and dissemination.

Record keeping has gone on since the Stone Age but record keeping techniques have grown and besophisticated ways of data gathering. There are, of course, many good reasons for collecting statistical and research data. These systems, however, also must be carefully safeguarded in order to protect the data subject from injury. In 1972, the then Secretary of Health, Education and Welfare, Elliott Richardson, created a citizen's Advisory Committee on automated personal data systems and I was appointed a member of that committee. The committee encompassed a broad range of expertise and experience and equally diverse range of viewpoints.

Given this diversity, it should be no surprise that at our first meeting, in the spring of 1972, the views of individual members on the significance of applying computer technology to personal data record keeping, sometimes differed sharply. Many, indeed probably most, did not initially feel a sense of urgency about the potential ill effects of current practices. Some agreed that computer based record keeping posed a latent danger to individual citizens, but looked optimistically to technical innovations, particularly access control devices. Others painted dramatic portraits of the potential benefits of large scale data networks to citizens in a densely populated, highly mobile society.

Slowly, however the attitudes of the members changed. Shared concerns took root as we heard testimony from over 100 witnesses representing more than 50 different organizations. The danger that individuals without knowledge or warning could be harmed and harrassed by an unthinking machine came out in the light of day for all of us to see. We were not the only ones concerned with this topic.

In an article published in the February Issue of "Barrister Magazine," Senator Sam J. Ervin, Jr. discussed his investigation into the computerized collection of personal data by the Federal Government. He indicated that, at the present time, there are at least 750 separate data banks with varying contents and operational guidelines within the Federal Agencies. 750 separate places where a citizen's name, address, occupation, family history or countless other bits and pieces of information about his life may be stored, and more importantly, 750 different opportunities for such information to be used in ways completely unknown and objectionable to the subject or to be disseminated without the subject's knowledge or concent.

Further, the information may not even be correct. Senator Ervin reports that in one system, there was a numbered coding system to indicate whether an individual was or was not a Communist and that the number code indicating an individual was a Communist

was only one number different from that indicating non-Communist. Were any of those codes incorrect? The Senator wonders and so do I. For the consequences of disseminating such erroneous information would be horrendous on an individual's career and life.

It concerns me, as a mother of a daughter who has attended college during recent times. Is it possible that she might have been seen standing innocently near a gathering which turned violent and someone noted in a file somewhere that she was an active participant? An error could have been made and somewhere a computer could contain such erroneous information which will prevent her from being employed or obtaining credit. She has no way of knowing, nor do I.

An error of observation or a mistake in coding could, through improper dissemination, destroy her life without any sort of attendant guilt or her part. Do any of us know in which data banks our names might appear or what information about us is stored away by such machines or, finally, what uses are made of the information?

Clearly, the dangers indicated require that action be taken for our protection. The final question then becomes: What action? The committee on which Senator Aronoff and I served, made several specific recommendations. Senator Ervin's subcommittee on constitutional rights has made others. I would not attempt to list the various proposals suggested nor to read the list of legislative measures which have been proposed, for my purpose here today has been to discuss the problem from the point of view of the individual citizen. All of the proposals require our careful consideration, however, and more importantly, the careful consideration of the Congress.

Mr. Justice Brandeis spoke of the problem in the 1928 case of Olmstead versus the United States when he said:

> "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning, but without understanding."

I am hopeful that now, 46 years later, positive action will be taken for protection of rights so long and flagrantly abused by those who govern us.

THE ISSUES OF PRIVACY AND COMPUTER SECURITY WITHIN THE STATE OF OHIO

Stanley J. Aronoff
Ohio State Senator, State House, Columbus, Ohio 45215

Thank you very much, Arthur. You ought to know from the Harvard faculty that there's nothing more virtuous than a convert and I freely confess to being just that. That was my function, at least for 14 of the 23 meetings of the HEW Committee. For some period of time, after each witness that came forward, I generally asked the question. "What's all the fuss about?" "What are we trying to hide?" Or, "you haven't scared me yet."

Some place around the 14th meeting, I noticed a big change in my own questioning technique and by the end I was raving for action and demanding that there be a shield of privacy that each of us may use and have if we get stored in the bowels of the computer.

I might say in starting out that I am anti-technology or anti-computer. Frankly, I can't envision any modern life without the sophisticated use of computers. So, it's merely a balancing act that I'm interested in. An act that protects an individual's rights on the one hand and does not inhibit the justifiable use of computer technology. I realize I have a very learned audience and I hope you won't consider me totally boring if I identify for you in very short form what is listed in the HEW Report. If you're going to have a Code of Fair Information Practice, then you have to start at the beginning and identify what are the unfair information practices that are going on now that promote such a code. Do they justify the kind of strict legislation that I hope you will be an advocate.

Number One: *The unfair information practice of getting too much information.* Here are some of the examples that we get out of the Committee after hundreds of hours and mounds of testimony. Take the Credit Bureau as an example. We all know the necessity for credit; we all know that there are computer banks storing credit information, the largest one being in Atlanta. But, aside from the earning capacity, is it necessary for the neighbors to be asked whether an individual entertains at late parties, drinks, takes drugs, and all kinds of information such as that, subjective information, which then gets stored into the computer even though it's hearsay? We had an example of a man in New York who had his insurance cancelled because his son had long hair. Because the son had long hair that meant to the neighbor that everybody was on drugs in that family, they were "bad risks"! Therefore, the insurance company cancelled and it took a period of time for the man to get his insurance back. Annoying, but something we should all consider after we look at our children, or look at ourselves.

Or examine the guaranteed student loan program. The purpose of that program is to give money to needy children in order for them to get an education.

But in one state which testified before the Committee, other questions were asked, such as, "project your grades," or "project the kind of sex activity that you'll be getting into at the University." Well, what does that have to do with a guaranteed student loan program; and when we asked the interviewer why the question was asked, she just said, "I thought I'd like to know about that." There's no way of stopping that kind of "I'd like to know about" on questionnaires that are prepared countless times in all kinds of professions and Government.

Unfair information practice Number Two: Using information for purposes other than those for which it was originally gathered. There was an example that came before the Committee of a man that walked into the home of a young GI just after he had gotten out of the Vietnamese war, reached into his pocket and flicked out an envelope. When the young GI picked it up and opened it, there was $10,000. Well, $10,000 for what? This man was being contacted and given $10,000 in order to kill an underworld figure. He was being contacted by organized crime in order to become a contract killer. Why? Because somehow they had gotten hold of his army record and found that this guy had been involved in a number of "kills" in the Vietnamese War.

What about the simplest example that happens to us all—junk mail. I am a politician in the State of Ohio. I received this in the mail last week (showing exhibit). "Senior Citizen. Computerized mailing list of over 7 million over-65 adults." It was compiled from all kinds of things: medicare policies, adult retirement, and it goes on for a few other things; then it says, "marital status: couples only, widows, etc.; home ownership, retirement income level; age and date of birth in selected States"; and finally, "five digit zip codes on test orders under 10,000 names"; then in yellow underlined and I did not do this: "political campaigns for use of senior citizen voters." (Arthur, you might want to use this in the next compilation that you have.) Again, we all are victims of junk mail. Some of it we like and some of it we don't. In the State of Ohio, I raised holy hell because the State was proudly saying that when you go to buy an automobile license each year we take your name and we sell it. Well, terriffic! The State of Ohio made $65,000 that way and then from that point on, somebody else owns your name and you get advertisements for this kind of thing for your new car and that kind of thing for your new car; and they, in turn, sell the list to somebody else and ultimately you have the progression here. The State of Ohio no longer does that.

Unfair information practice number three: Using incorrect or incomplete information. Here I think we have the example of the arrest record which has been talked about over and over and over again, and I merely would say that the statistics that came before the Committee indicate that a substantial percentage—and I forget the exact percentage but I know it was shocking—all youth under the age of 25 will have been arrested and charged with a crime. Yet a great majority, a preponderant majority, will not even make it to court. The question is do we want correct records! I think what's going on in Washington gets at that point.

But I think another more tragic type of example is one where a young person had just recently gotten out of the war. He and his wife, after a long conversation, had decided to adopt a young child from a foreign country, until the report came back that this fellow was "morally unfit." Why was he morally unfit? He had been labeled a "heroin addict" on his way out of the military service. Now I don't know if you all remember when you were discharged from the Army, but I remember the mustering out process and some of the guys that were doing it, and I ask you whether it's possible that somebody in that line might make an error and label someone a heroin addict when the person was not. It obviously is possible and in this case it happened and it took the Red Cross a year to solve the problem and there were still problems in a Domestic Court thereafter.

A fourth unfair information practice is: being haunted by paper ghosts of the past. In 1974, the idea of "Go West, young man and start a new life" is ridiculous. Your records get there long before you do. We can't escape to your State anymore, Mr. Cullen. If we try to leave Ohio, or Massachusetts, you'll catch us out there or the record will.

And we had an example before the Committee of a person who did not accept promotion in a rather large retail chain. This man was black, and it would have been a good promotion. But it would have meant revealing a minor misdemeanor on the east coast some 25 years before. The problem that he had was that it might have cast some disparagement on his race when he was reaching a high level. The question has to come up whether there should be some statute of limitations on stale information.

And finally, I suppose the most important of the *unfair information practices, the denying of an individual, the denying of you and me of the effective control of our record.* I guess the simplest example that we all have is when we take an insurance examination. We get an examination from an insurance doctor. Before going to the Committee, I was naive and thought that that was an examination just for that insurance company; I didn't realize that it was stored in a master bank. Although the insurance industry has told me countless times since then that one company or another company never has an opportunity to look into that bank. If a person has been denied coverage by one company and the other company knows it, I ask you whether or not that has some bearing. But more importantly, you don't have an opportunity to look at your medical record if you are stored there. (Note, this has now been changed.) And I think that's the key. If there's nothing to be afraid, when why shouldn't you have a chance to look at your record and see if there are some corrections that should be made.

The 55 mile speed limit will catch us all from time to time. It used to be that when you were stopped for speeding, your friendly police officer came up to you and said, "Now, Stan, you're going a little fast" and

you have a conversation back and forth and you usually got the ticket anyway after you tried to talk him out of it. That's not the case now. Now you're stopped. You give your driver's license with your social security number. The police officer goes into his car and he dials the regional computer center of a certain area which in turn plugs into Washington and then back it comes with your record. Not only your automobile record, but your whole criminal record. And instead of catching Arthur Miller, you may get "Jack the Ripper." And law enforcement officers are very proud if they catch somebody by doing that. But what about the incorrect record and the problem that these are collected from local governments the theory of "garbage in, garbage out."

Well, I think I've talked enough so that I at least ought to get to the bill. And the bill I've introduced into Ohio is very similar to the Congressional bills that you heard. It is similar in other respects to the California bill, but I hope it has some individuality of its own. I hope we'll have a chance of its passage.

On the one hand, it describes individual rights. What rights do you have if you get into a computer? And i describes them. You have to be informed in writing if you're legally required to give the data. You have to be informed in writing whether you're the subject of the data in a system and, upon request, that data must be made available to you. You have to be assured in writing that no use of the data will be made beyond the stated purposes of the system as reasonably understood by you. You have to be informed upon request of the uses made of the data concerning you. Procedures to allow you to contest the accuracy, the completeness, the pertinence and the timeliness of the data must be made and the bill outline a procedure to make corrections.

And finally, although I do not know whether this will remain in the bill, it prohibits the use of the social security number unless specifically authorized by Federal law.

On the other hand, there's a set of do's and don't's for computer managers—a kind of "code of ethics." First of all, every person or firm operating an automated, personal data system must file with our State of Ohio in a designated agency a statement of purposes and uses of the data system; must obtain the prior informed consent of an individual—you—before making use of data, must appoint one person responsible for the security in information in the system and inform all employees using the system of safeguards established pursuant to the act; specify disciplinary measures to be applied against anyone who is discouraged from reporting if something is wrong; take precautions to protect the data from unauthorized use; make no transfer of individually identifiable data to another system without the prior consent of the individual concerned; maintain a complete, accurate record of every access and use made of data in the system; and maintain the data in the system with such accuracy as to fairly reflect the individual's current qualifications and characteristics. Finally, eliminate the stale data.

The act gives civil and criminal penalties, injunctive relief, and a variety of court actions that say, in effect, that these are not just words written by the Ohio legislature; but if a person has been aggrieved, then that person has a method for redress.

It's tough stuff and hearings start next Tuesday. Some of the people here are going to be witnesses I believe and I hope to be able to come back to you and give you a progress report.

Thank you.

THE ISSUES OF PRIVACY AND COMPUTER SECURITY WITHIN THE STATE OF CALIFORNIA

Assemblyman Mike Cullen
California Assembly, Sacramento, California 95814

In November of 1972 California voters responded to the question of protection of individual privacy by amending the California Constitution to include privacy as an inalienable right of all people.[1] By that action the people of California were providing their legislature with a very clear message which reflected a general dissatisfaction with the erosion of the personal privacy.

They had come to the sudden realization that, like the bald eagle and the peregrine falcon, privacy was itself an endangered species too easily taken for granted. It had been allowed to dwindle to the degree that it had become more of a concept than a reality. And just as the eagle and the falcon are integral parts of our natural ecology, so is privacy an integral part of our social ecology, and the people of California are asking that the assault on it be halted.

We in the California Legislature have responded to that mandate and have taken, and are in the process of taking, a number of steps which will assure that the privacy of Californians does not become a myth.

One of the more pervasive elements in the assault on privacy has been the increasing employment by government and the business sector of electronic data processing (EDP) technology. The California Legislature has focused on the uses (and abuses) of this technology in its attempts to come to terms with the issue of privacy. It is apparent that the right of an individ-

[1] California Constitution, Article 1, Section 1.

ual to privacy is contingent on a modern day factor, that is, computer-related security. Neither constitutional assertion of privacy as a right nor statutory reaffirmation of this right will enhance its chances for survival unless provisions are made for security of data which is contained in automated systems.

California's long time pioneership in governmental application of EDP technology has provided our legislature with the background to cope with EDP. The State's commitment in this area is evidenced by an annual expenditure of $135 million attributed to computer-related costs (and these costs keep rising). This figure excludes the millions of Federal dollars spent on computer services in health, welfare, criminal justice and the California University Systems.

In retrospect, the California Legislature's long standing and active interest in the development of EDP systems in State Government has served to equip it with sufficient understanding to enable the legislature to respond quickly and realistically to the issue of privacy in EDP applications.

For some years, the budget enacted each year by the legislature has contained in supplemental language the requirement that the pursuit of maximum EDP effectiveness in State Government" . . . not jeopardize or compromise the confidentiality of information as provided by statute or the protection of the right of individual privacy as established by law."[2] The key is, of course, the dependence on established law.

As California's EDP representative to the National Conference of Legislative Leaders, I have shared my experiences of 1971–72 where I was the Assembly representative on a joint California Legislative Committee that developed and painstakenly nurtured through both houses urgency legislation,[3] passed in 1972, providing for State Information Security Officers. The legislation also served as a basis for requirements added by the legislature in supplemental language to the Budget ACT of 1972. This language required that (1) designers of information systems include in their analyses the recognition of the use of confidential information; (2) strict controls be developed to prevent unauthorized access to data maintained in computer files, including the physical security of program documentation, data files and data processing facilities as well as electronic controls to prevent accidental or intentional unauthorized access to data, (3) each state department designate an information security officer responsible for implementing state policies and standards regarding the confidentiality and security of information for that department, (4) the Department of Finance (which has statewide control of EDP in California State Government) continually review the adequacy of State policies and procedures with regard to confidentiality of data and report to the legislature on progress in this area, and (5) any contractor engaging in EDP-related work for the State must agree in appropriate contractual language to hold confidential the details of the work performed. We stipulated also that any EDP-related contract entered into by any State entity provide for the contracting staff to be physically on the premises of the data center or State entity concerning systems design, programming, documentation, conversion, training and all other aspects for which the contractor is hired. Further, because California is moving in the direction of consolidating our EDP resources into five large-scale consolidated data centers, we required that each consolidated data center also designate an information security officer; that the RFP for each center contain mandatory objectives to be placed on the vendor in the areas of confidentiality and privacy. Legislative review of the RFP was a requirement prior to issue.

As a direct result of legislative concern over the enhancement of the assault on privacy made possible through electronic means, the 1972 Legislature also added supplemental budget act language which prohibited the transmission of data from one data center to another by any wire, line or other communications device. The one exception allowed has been the transfer between two data centers of stolen vehicle information for law enforcement purposes.

The Legislature's 1972 decision to consolidate the State's computers into 5 Data Centers has caused concern. However, it is the consensus that, through data consolidation, protection of privacy will be improved through systematic control over all phases of security for each center. In one of the State's consolidated data centers, it is expected that more than one billion input/output calls will be made each year. Much of the information will concern personal data associated with organizations such as the State Personnel Board and the Employees Retirement System. The biggest problem is to equate privacy protection costs to realistic operational costs. Regardless of the ultimate protection afforded in each of the Consolidated Centers, the constant recognition of the protection of personal privacy should keep the personnel involved with systems operations alert.

These actions taken by the legislature have in turn caused the Executive Branch of California State Government to take action to implement the legislative mandate. For example, we now have information security officers in State departments and in consolidated Data Centers. We now have in the process of development an EDP facility auditing program of which an integral part is the auditing of EDP security and confidentiality. We now have continuously updated security guidelines and checklist package for use by State Agencies in the establishment and maintenance of appropriate safeguards for the physical and confidential protection of data. Most importantly, the full attention of the legislature has been directed toward this most vital area. This attention must continue because the relative inexpensiveness now associated with the collection, manipulation and dissemination through electronic means of inordinately large amounts of personal data has effectively removed the economic

[2] "Supplementary Report of the Committee on Conference relating to the Budget Bill" (beginning with the 1970–71 fiscal year).

[3] SB 1503 (Teale 1972), California Government Code Section 11775–11785.

constraints imposed by manual systems which had previously precluded most of the "data handling" capabilities which we now are concerned with.

Our most current effort in the area of privacy, which, has generated interest nationwide, is reflected in Assembly Bill No. 2656 (AB 2656). This measure would enact the California Fair Information Practice Act, the provisions of which parallel closely the recommendations contained in the widely read report prepared for the U.S. Department of Health, Education and Welfare (HEW) entitled "Records Computers and the Rights of Citizens."

In fact, AB 2656 recognizes in its provisions the five basic principles which form the basis for the HEW report's recommended code of Fair Information Practice. As stated in the Bill, the California Legislature recognizes these principles to be:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for an individual to find out what personal information about him is in a record and how it is used.

3. There must be a way for an individual to prevent personal information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

4. There must be a way for an individual to correct or amend a record of identifiable personal information about him.

5. An organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

The measure has already passed its house of origin, the assembly, and is now pending in the senate. Because it is still in the legislative process, it is naturally subject to further revision. Its introduction has generated a considerable amount of interest in the California business community and also in the State and local Government sectors. This interest and concern may influence to a degree the final version of the measure. In this regard dialogues have been initiated between our legislative staff and various interested groups in order to make appropriate clarifications to the measure.

Because I have brought a sufficient number of copies of the current version on the bill for distribution, I will just touch on its highlights in my presentation to you. To begin with, the provisions enumerated in AB 2656 apply to both governmental and nongovernmental automated systems which contain personal data (which is defined as ". . . any information that describes anything about an individual and which can be associated with an identifiable individual"). This is a rather all-encompassing definition and may explain why the measure has generated such widespread interest within the State among groups that would be affected by enactment of its provisions. Simply put, AB 2656 will leave no stone unturned in terms of the protective umbrella it would provide for our citizens. It would affect a good number of organizations in California because it is not seen as some sort of halfway measure, but one which will provide an appropriate level of response to the people's mandate when they voted to amend the California Constitution in 1972 to include the right to privacy as an inalienable right.

Now, to get on with the specific areas provided for in AB 2656, the measure stipulates requirements placed on those maintaining an automated personal data system for the safeguarding of data maintained in such systems. These requirements include (1) identifying one individual immediately responsible for the system, (2) the instruction of appropriate employees regarding required safeguards, (3) reasonable physical, technical and procedural precautions to protect data in the system from any unauthorized release, transfer, access or use, or any threat or hazard to the security of the system, (4) the establishment of safeguards regarding the transfer between systems of individually identifiable personal data before any such transfers may take place, and (5) the elimination from a computer-accessible form of obsolete data.

Secondly, the bill requires that those maintaining an automated personal data system give annual notice of the existence and character of the system. This notice must be filed with the California State Department of Consumer Affairs as a permanent public record, must contain a number of specified informational items including the procedures whereby an individual can be informed if he is the subject of data in the system, and if a subject, how he can gain access to such data and contest its accuracy, completeness, pertinence and timeliness.

Thirdly, the measure provides for the rights of individuals on whom personal data are maintained. These rights include the requirement that an individual asked to supply personal data must be informed in writing whether he is legally required to supply the data requested, of any consequence which may arise by his permission or refusal to supply such data, and of the uses to which such data will be put. Further provisions in this area require (1) that an individual be provided, in writing, at his request, information which discloses whether he is the subject of data in the system in question, and if so, that such data be made fully available to the individual in a form comprehensible to him, (2) that no use of individually identifiable personal data is made which is not within the stated purposes of the system as reasonably understood by the individual at the time he was asked to provide the data, (3) That no data about an individual are made available from the system in response to a demand for data made by means of compulsory legal process unless a reasonable effort has been made to notify the individual in question, and (4) that procedures are maintained which allow an individual to contest personal data maintained on him, and, where the contest is not resolved favorably, to provide that whenever disputed data are disclosed such disclosure clearly note this fact and a copy or accurate summary of the individual's statement in this regard be provided with the data.

In the way of "teeth" with which to ensure compliance with the various provisions of AB 2656, the measures contains penalty provisions which include fines, imprisonment, and punitive damages for specific violations.

In summary, we believe that the Bill will provide a meaningful response to the mandate of the people of California, that it is comprehensive, and that amendments made to date have not detracted from the measure's original intent, but have in fact made it a progressively better piece of legislation by providing appropriate clarification.

Another piece of current legislation which has yet to be heard before committee has also been introduced in the California Assembly. This measure, Assembly Bill No. 2802, would stipulate some requirements regarding the use of the Social Security Number. Unlike AB 2656, the provisions of this measure apply to all transactions; that is, they are not restricted to the use of the Social Security Number in EDP systems only.

In brief, this Bill would require that any person who makes necessary the disclosure of an individual's Social Security Number as a part of a commercial or governmental transaction report the fact of such requirement to the Department of Consumer Affairs, which is to maintain a record open for public inspection of those persons reporting.

The measure also requires that an individual asked to provide his Social Security Number as part of a commercial or governmental transaction be informed whether such disclosure is necessary or optional, and permits an individual to have his Social Security Number removed from records where disclosure of the number was not necessary.

Further provisions of AB 2802 would make unlawful any requirement of disclosure of an individual's Social Security Number for personal identification in governmental or commercial transactions unless specifically authorized by Federal or State law.

Because AB 2802 has only recently been introduced, it is difficult to tell at this time whether or not it will enjoy the same degree of success that has been the case to date with AB 2656.

Now, looking at the issues of security and privacy from yet another aspect, I would like to discuss some further action that has been taken by our legislature in this regard. In California, as in other states, there is data exchange and data sharing between the State and local governmental entities and among local entities themselves. Recognizing these data transfer "linkages," the California Legislature has enacted legislation creating an Intergovernmental Board on Electronic Data Processing. This Board monitors the development of State and local EDP systems which will exchange information, with the objective of assuring that the duplication of systems development is avoided, and that appropriate communication takes place among the various governmental jurisdictions participating in the development of such systems.

The Board has also been given specific statutory responsibility to ". . . recommend any legislation required to insure the protection of individual privacy and the necessary confidentiality of information becoming part of an intergovernmental information system."[4]

The Board, which receives a nominal amount of direct State funding, derives much of the productivity through volunteer effort contributed by the State and local Government entities as represented by board members and technical staff. The Board has established a privacy and security committee which, in addition to working in the area of legislation, has published just recently a report of the Board entitled "guidelines establishing requirements for security and confidentiality of information systems." With 58 counties, almost 400 cities, and 1,124 school districts (not to mention 3,000 special districts), the efforts of the Board as reflected in the guidelines will be of especial value to the smaller and emerging governmental users of EDP technology, although it is accurate to state that there is also considerable room for improvement also in some of our large EDP facilities. For those interested, I have sufficient copies of the guidelines table of contents and procedure for ordering the publication.

With regard to the area of computer security, I would like to discuss for a moment a relatively recent occurrence in our State which brought very much to home the question of computer security—but in a somewhat different light. Incidentally, this occurrence demonstrated clearly the willingness of the California Legislature to meet the security issue head-on and take appropriate steps to resolve the issue which confronted it.

In 1973 California and certain other States received much national recognition with regard to a particular incident in the business community. I am referring to the so-called Equity Funding Scandal as you may recall. This was a situation where the Equity Funding Corporation of America was found to have perpetrated a considerable degree of costly fraud through the use of company computers.

Once the nature and extent of fraud had become evident, our reaction in the California Legislature was to (among other things) augment the budget of the State Department of Insurance to provide it with sufficient funds to acquire a high-level technical expert who possessed expertise in the insurance and computer fields in order to develop within the department of insurance the ability to audit effectively EDP systems maintained by insurance companies.

Because we have for the most part centralized EDP training within California State Government, we have been able to develop with the Department of Insurance expert a training program which should greatly improve the ability of that department to perform more effective auditing of systems maintained by insurance firms.

This is somewhat of a different twist on the computer security question. In this case, while we want insurance company systems to be secure with regard to the confidentiality of personal data maintained by

[4] California Government Code, Section 11711, Subsection (f).

them, we want our department of insurance auditors to be capable of determining to the maximum extent possible when the computer is being used for an illegal purpose.

In conclusion, I would like to focus on my own experience over the past year as well as my thoughts for the future. While chairman of the Assembly efficiency and cost control committee, the committee over the past three years has heard all electronic data processing bills including the Fair Information Practices Act of 1973 (AB 2656) discussed earlier. Also during 1973, the committee conducted four public hearings concerning computer privacy and security. In addition, I have been appointed chairman of joint legislature subcommittee to develop the plans and goals of legislative electronic data processing. Our report will be promulgated April 15 and will include plans for sharing executive files without violating either privacy or security. Also, I am participating as chairman of a unique high-level executive legislative statutory committee[1] called the California Information Systems Implementation Committee consisting of the directors of finance and general services representing the executive and the chairmen of the Senate and Assembly Finance Committees, the chairman of the joint legislative budget committee and myself as chairman of the efficiency and cost control committee. To insure nonpartisanship, the Vice Chairman of each Legislative Committee is also a member at present. The Committee is actively pursuing its statutory charges of (a) reviewing electronic data processing policies; (b) developing electronic data processing procedures to protect privacy and confidentiality of records and rights and privacy of the individual; and (c) reporting recommendations to the Legislature and the Governor. Through the hearing process, the committee is generating positive and immediate reactions from the nine campus university and 19 campus university and college systems and the State's vast communication networking systems in the areas of effective electronic data processing utilization and protection of information collected and transmitted.

California with nearly 21 million population and the business interests associated with this large population has experienced extreme difficulty in encouraging the utilization of computers while protecting the privacy of individuals and insuring the security of data. Through the three committees that I have mentioned, plus the past pressure-filled five years of legislative maturity in the computer environment, I feel California has established a privacy and security umbrella which is still a leaky one but at least supported by bits and pieces of statutes addressing privacy problems. I am optimistic that by the time the California Legislature adjourns on November 30, 1974, the progress made through legislation and the momentum for safeguards established with the private and public sectors, may well assure the people of California that the word "Privacy" in their Constitution is a meaningful one now protected and ready to be defended from further unforeseen circumstances.

[1] AB 644 (MacDonald 1973), Government Code Sections 11755-11758.

THE ISSUES OF PRIVACY AND COMPUTER SECURITY WITHIN THE STATE OF MASSACHUSETTS

Arthur R. Miller
Harvard Law School, Cambridge, Massachusetts 02138

It is very fashionable to think of California as one of the legal pacesetters of the nation. It is true that they did enact a constitutional amendment inserting privacy into their constitution at their last general election. Montana has done the same thing. If memory serves me right, at the same time that the people of California were voting for privacy, they were also voting for the death penalty, against marijuana and for pornography. This combination suggested an interesting profile of the California voter. I, too, come from a unique state—Massachusetts. As I indicated earlier this morning, I am originally a New Yorker, I have been a Minnesotan; I have been a Michigander; and for short periods of time, I have been a Floridian and a Californian; but I am now from Massachusetts. Massachusetts has a long, but somewhat checkered, legal tradition. It started with the Salem Witch Trials; proceeded through the Sacco Vanzette incidents; and its most recent manifestation was the trial of Dr. Spock and Reverend Coffin. Seriously, however, we do undertake some rather interesting things in Massachusetts.

One aspect of Massachusetts law that is interesting and which I have been asked to speak for a few minutes on, is that State's recent reaction to problems of privacy. We have a Republican governor, Governor Sargent, who takes great pleasure suing a Republican national administration. You heard something about that earlier this morning. It took the form of a petition against the Department of Justice challenging the FBI policies with regard to the National Crime Information Center files. Conversely, the Republican administration in Washington is fond of suing the Commonwealth of Massachusetts, which they did last year in trying to get access to the Massachusetts criminal history files.

A great deal is going on in Massachusetts in the privacy arena. There are three things worthy of special note. First, Massachusetts was, I think, the first State in the Union to legislate with regard to computerized criminal recordkeeping. A statute was passed in 1972 that is designed to manage what is called criminal offender record information that will be in a fully automated criminal justice information system that will service all of the law enforcement agencies in the Commonwealth. This statute created two administrative units. One is the Criminal History Systems Board, which has operating control over the criminal justice information system. It is a regulatory body composed of representatives of the data users—law enforcement officials, rehabilitation officials, and court officials. It is an in-house professional group. In addition to the Board, there was created a Security and Privacy Council consisting of nine members, seven public members who work on a *pro bono* basis, and representatives of the Attorney General's office and the chairman of the Criminal History Systems Board. I serve as chairman of this Council. The Security and Privacy Council's function is to study, monitor, audit, and present recommendations to the Board with regard to matters bearing on security of the system and the privacy of the criminal justice files. It really has no power—none whatsoever—other than the power of recommendation. All power resides in the Board. Fortunately, the Council seems to have captured the good will of the Board and the two organizations are working in reasonable harmony.

In the period between the enactment of the statute and the present, very, very detailed regulations have been drafted by the Board with the advice of the Council. These deal in great detail with regard to such matters as security of data, access to data, dissemination of data, the purging and sealing of data. Anyone interested in seeing a fully developed regulatory system would be well advised to look at the regulations proposed for the Massachusetts criminal justice system. In my judgment, it represents a rather reasonable balance between the needs of the law enforcement community and the rights of the individual, although I do not agree with everything in the current draft. Of course, these regulations are reinforced by a strong statute that prohibits the movement of criminal justice information outside the criminal justice community and those governmental organizations authorized by statute to have access to criminal justice information. If properly enforced, this is a very limiting standard. There is no legal way an employer, an insurance company, or a credit-rating or credit reporting agency will be allowed to gain access to the Massachusetts criminal justice system.

The second development in Massachusetts is the appointment by the Governor of a Commission on Privacy and Data Protection. In many ways, this Commission is modelled after the HEW Committee. Its charge is about the same and its composition reflects the same wide angle of experience and expertise that characterized the HEW group. It is a commission composed of private citizens who are not compensated. I serve as its chairman. We are just getting underway by investigating the state of recordkeeping in Massachusetts, the level of security that exists, the amount of technological attention being given to matters of privacy and security. We expect to take testimony from citizens and to respond to individual complaints. We already have started to receive them and they follow the usual pattern of objections to the use of the social security number on driver's licenses, the lack of file security in welfare offices, the selling of lists of customers or members to consumer reporting and mail list companies.

The third development in Massachusetts symbolizes what I said earlier this morning when I suggested that the privacy issue has come of age. The computer-privacy issue has the enormous political sex appeal. Not to be outdone by the Governor, the General Court of the Commonwealth of Massachusetts, which is its legislature, has appointed a commission to study privacy. Of course, its efforts will be largely duplicative of the Governor's commission, although it probably will be more action oriented because it is composed of nine State representatives and three public members. It, too, is just underway in its work.

I have described the Massachusetts scene simply to indicate to you that considerable activity is going on at the State level and the object will be to place a bill before the entire legislature. The executive and legislative branches of dozens of States already have become active in trying to deal with this problem. One of the really significant problems that face policymakers, in particular those at the operating levels of government, such as many of you people, is to avoid the zealots, both the zealots of government efficiency on the one hand and the zealots of civil liberties on the other. Unfortunately, many of the proposals that are appearing are technologically unsound, administratively unworkable, or placebos that really accomplish little because they offer people no effective procedural mechanism either in terms of gaining access to their files or in terms of challenging inaccuracies in the file. If there is a single important role for governmental policymakers, it is to help the legislators find a mid-course between the extremes; otherwise we will end up with extremely bad legislation. I think you must face the fact that given the appeal of the privacy issue, there will be legislation and the real question is how good can be make it.

THE VIEWS OF THE COMPUTER AND BUSINESS EQUIPMENT MANUFACTURERS ASSOCIATION (CBEMA)

Peter F. McCloskey

President, Computer and Business Equipment Manufacturers Association
1828 L Street, N.W., Washington, D.C. 20036

Thank you and good afternoon. As noted already, President Nixon has increased dramatically the importance of our deliberations here, and I hope that there are some staff members from the Domestic Council with us because the issues raised at the November Conference and addressed again at this one cover most of the issues before Vice-President Ford's Committee. CBEMA has long believed that society must set the rules for privacy so that administrators, systems designers and equipment vendors can implement the confidentiality rules and security systems to preserve that level of privacy. In this context, I have three conclusions to discuss with you this afternoon.

First, Information Protection: Information can be protected better in a computer system than in a manila folder.

Second, How Much Security Is Needed? Security expenditures must be based on cost benefit analyses. The extent of security measures depends on the assets to be protected and the perceived risk.

Third, How Much Security Is Available? Better security products are coming in response to perceived market demand but I must note that government demand seems to be well ahead of other markets.

Last November this conference addressed issues facing the government manager regarding Privacy and Security in Government Computer Systems. I reflected on the views stated at that conference during my return from East Europe and the USSR last week. It is very clear that those are societies in which information is secure. And, it is just as clear that it is not the use of computers that determines the character of a society.

Franz Kafka in his novel "The Trial" found little need for a computer to ensnare his victims. In the United States and other Western nations, however, the computer is beginning to be cast as a villain. I don't agree. I agree with Alan Westin, who sees the computer as the catalyst causing a reaction between long established trends towards Institutionalization and Meritocracy on the one hand and new concepts of personal freedom and group dignity and rights on the other hand.

In this connection, the Canadian Government Report: "Privacy and Computers" notes that not all claims to privacy fall within any reasonable concept of privacy. The demand for access to personal files can also be seen as an attempt to alter the distribution of political power. And, the arguments about "computer errors" are essentialy arguments about defamation—even if the context is new.

These are genuine concerns, but how can we best address the range of issues before us? I believe our society must look at Privacy, Confidentiality and Security of information from a systems viewpoint. In this examination different concepts are needed at different levels and various groups play different roles.

CBEMA has been actively concerned with the expanding impact of data handling techniques on society for many years. As awareness of these developments grew within the Industry, we established a Committee on Privacy and Security. Through this committee, CBEMA has followed closely the growth of interest in the Congress, other legislative bodies, the Executive Branch of the Federal Government and in the States in the subject of Governmental use of information technology. We therefore, welcome the opportunity to participate in conferences such as this since one of our activities is to promote informed public discussion of the part data handling techniques, and computers in particular, play in the collection and administration of information about people.

Our recently published CBEMA statement, "The Role of Computers in Privacy, Confidentiality and Data Security," addresses the issues as we see them and copies are available in the auditorium. This statement is the first in a planned series of publications designed to stimulate thought and discussion. We have published the speech given by Ruth Davis at the November Conference. We think Dr. Davis provides a thoughtful overview of this issue as a concerned Government Official. We are distributing this speech to the Congress, State legislatures, the Federal and State Executive Branches because we think it's important.

The activity of the CBEMA Commitee on Privacy and Security is based on two convictions:

- Preservation of the individual's right to privacy is a fundamental goal of our society.
- The use and advancement of information processing techniques are vital to solving the problems presented by our increasingly complex society.

Concern for privacy is not a new subject. Since the beginning of recorded history, there has been concern about the collection of information and its use as it affects individual privacy. Each age and society has continually reviewed the balance between the rights of the individual to be left alone and the needs of

society to obtain, use and disseminate data concerning him. Today's complex society and advanced technology gives this concern a new dimension. As we stated to the Federal Communications Commission in 1968:

> "It is pertinent to note that privacy questions involving stored data are not the result of the development of computer and data processing techniques. The increased concentration of data would have developed in any event, and the computer, while contributing to the immediacy of the privacy problem, has at the same time, contributed in major respects to our ability to provide for the secure storage and use of information."

Certainly, the computer, with its ability to process vast amounts of data rapidly and economically, has proved its worth to mankind. It also has complicated the effort to preserve the rights of the individual. We should remember, however, that Alan Westin reported to the November Conference in his global review of recent studies on privacy that none of the studies could document specific episodes where automated record-keeping created a new loss of personal liberties. During the past ten years, the growth of computers has been impressive.

In 1961 there were less than 20,000 general purpose computers installed in this country. Today there are over 60,000. In the Federal Government alone there are currently over 1,000 general purpose computers installed whereas ten years ago the number was less than 2,000. Now, the total number of CPU's installed is much greater, but we are looking at those systems that are most likely to be used to process personal information.

In addition, a recent Kiplinger Washington Letter, indicated that the biggest growth industry in the United States during the next ten years will be public service. Government at all levels will grow rapidly, particularly State and Local Governments. We believe that this anticipated growth in public service will result in the continued application of computers to effectively handle the data this is vital to Government operations.

In an era when organizational judgments about people affect many rights, benefits and opportunities, this projected growth highlights the need for continuing review. The key to an effective approach to resolving this concern is understanding that three intertwined aspects of these issues exist: Privacy, Confidentiality, and Data Security.

The overriding consideration, of course, is an individual's right to *privacy*. This right involves such basic policy questions as: What personal information should be collected? By whom? For what purposes? Who should have access to what information? For what purposes? Under what limitations? The problem of preserving privacy was with us long before computers came on the scene. It has existed since people started keeping written records.

Confidentiality on the other hand involves the treatment of personal information after it is on file. An individual may wish to keep most facts about his personal life to himself. However, he may also be willing to give some confidential data to an agency or company to be used for agreed upon specific purposes, such as medical treatment, bank loans, insurance, or employment evaluation. However, the individual will want assurance that confidentiality will be maintained and that unauthorized use of the data will not occur. Making good on the promise of confidentiality requires a variety of human and technological safeguards.

The third aspect, *data security*, deals with means of assuring confidentiality—protecting data from unauthorized disclosure, modification, or destruction, either accidental or intentional. Data security encompasses the protection of all files, manual or computerized. It can take the form of physical protection of the files, a variety of administrative procedures, and technical safeguards in computers. As information systems have become more complex, data security requires additional measures to control access to files by those not in the central installation itself.

Resolving the issues of where policy and regulatory responsibility for private information in Government systems resides is facilitated by considering whether the issue is a case of privacy, confidentiality or data security. It is the traditional responsibility of the legislature to develop, evaluate and formulate into law the sound public policies needed by society, in this case to establish the balance between the individual's right to privacy and society's need for information.

Legislative policy setting is often complicated by the fact that privacy issues usualy occur as ancillary parts of legislation addressing other subjects. The data gathering and research sections of the Family Assistance Plan proposed in the last Congress are an example. It is also the legislature's duty to set the rules for confidentiality requirements and thereby guide the executive branch in its execution of the law. Our census statutes are a clear example of such an approach.

Out of the controversy and debate over public policies, several principles have become increasingly accepted.

When Government or private industry places personal data on file, the individual should enjoy maximum access to records containing information about himself. He should have the right to reach and check the accuracy and completeness of the record, particularly when it is used to determine rights, benefits or opportunities. He should have the right to contest the record in an appropriate proceeding.

When information is collected from an individual for a given purpose, the use should be confined to that purpose. If the collector wishes to use the information for an additional purpose, he should make that clear originally or obtain consent later for the new use.

The relevance of specific items of personal information should be established, or the items should be deleted from the file. The indiscriminate transfer of information on individuals from one organization to another should be prohibited.

Once requirements for confidentiality are established, safeguards for private information can be identified. CBEMA member companies, other industrial firms, concerned Government agencies, and academic researchers have been working actively in this area.

Consideration must be given to the entire security environment if effective protection is to be established.

Traditional sound and prudent business practices should apply for manual or computer recordkeeping. These include such basic and necessary items as physical security, appropriate personnel programs and guidelines, separation of responsibilities, provisions for checks and balances, accountability, and appropriate audit procedures.

Our members and others recommend a variety of safeguards. They have helped work out procedural techniques for improving confidentiality; increased awareness and provided education for users so they may apply appropriate safeguards. As you will hear later they are continuing to study data security under the user's operating conditions, with the aim of developing still more devices and techniques. They are also providing Government with technical counsel: taking part in professional forums, as well as in academic and sociological research, aimed at better understanding of the issues and problems.

The computer manufacturers' most direct contributions are in the development of safeguards that can be built into the computer system. These safeguards were defined in the November Conference as "self-protected" systems. I'm sure conference speakers will address specific aspects of the problem of constructing self-protected systems.

Since CBEMA's viewpoint covers all systems manufactured by all member companies, I must address this problem from a very broad base. But trends are quite evident.

First, I think security has become an accepted issue by computer professionals. In contrast to the situation of several years ago, many people outside the military requirements sector now see systems security as a primary design goal. Certainly this is the reason many of you are here today.

Second, the manufacturers have undertaken to incorporate appropriate security techniques and facilities into their standard product lines. Security product planning has been raised to high corporate levels in most computer systems companies and is therefore a serious commitment.

Third, there is developing a heavy concentration on self protecting computer systems. This is the natural result of our tendency as manufacturers and users of sophisticated technology to look to that technology to resolve difficult problems.

Certainly such sophisticated approaches are necessary. In some systems they are the only means of providing the required level of security. At the same time let us not lose sight of the risks to be protected against. Donn Parker in his study of "Computer Abuse" which was completed for the National Science Foundation last November, listed vandalism, information or property theft, direct financial fraud or theft, and unauthorized use or sale of services as risks to be faced. We should include natural disaster and accidental disclosures in this list also. Of these risks only theft or accidental disclosure of information relate to invasion of privacy. Parker reports 21 cases of computer abuse occurring since 1967 in Local State and Federal Governments facilities. There were:

5 Thefts of address lists
4 Vandalism cases
1 Manipulation of Checks
1 Confidentiality violations
3 Manipulation of payroll files and checks
2 Unauthorized sales of EDP services and
2 Vote counting frauds.

In 16 cases the main perpetrator was an EDP employee, in 5, another Government employee and in 3 they were outsiders. Assuming theft of address lists is not considered an invasion of privacy, we see that 4 our of 21 or 1/6 of these cases relate to privacy. Further, none of these cases involved manipulation of computer programs.

The point is that beyond the safeguard capabilities built into the computer system itself, basic data security is best provided by traditional protective measures. In the installation location this includes locked computer rooms, identification cards, fire and theft protection, and the employment of trustworthy personnel, particularly programmers and machine room operators. Professor Westin observes in his report for the National Academy of Sciences, which was based on actual case studies, that the basic physical and administrative safeguards are judged by their own management to be inadequately employed in many of the organizations surveyed.

It should be recognized that with the large number and variety of types of computers in Government, and because of the complexity and scope of installed applications, each user must review available security alternatives including cost-benefit trade-offs in order to determine appropriate safeguards that meet his specific needs. As managers of Government programs providing services to citizens, your primary objective is to get the job done within budget. We must not make information so secure that doing the job becomes impossible.

Speaking of balancing the job of providing government services against preventing invasions of privacy, we think the diversity of proposed legislation on the privacy issue should be looked at. Dr. Ruth Davis at the November Conference, recognized this problem. "In 1973," she said, "some seventy bills concerned with protection of individual privacy were pending in the fifty state legislatures. Passage of any significant number of these bills, along with passage of some of the bills introduced into Congress could easily result in an unacceptable morass of conflicting requirements on service industries, technology and regulatory or judicial organizations. Some national coherence must exist for any realism to be present in arriving at security in automation adequate to protect individual privacy."

So far this year, we have noted the introduction of more than 20 new bills in state legislatures. The proliferation of bills being introduced dramatically points

up the need for a clear understanding of the benefits versus the cost trade-offs to be obtained. All interested parties—Government, user organizations, manufacturers, other concerned organizations, and individuals need to examine, study and understand this subject. Those concerned with privacy, should recognize that the really sensitive information usually exists in manual files, therefore, legislation must consider both manual and automated records. Negative information is just as damaging whether it is obtained from a computer or the familiar manila folder. This is one point that must be fully understood by Vice President Ford's newly activated Committee on Individual Privacy.

It is CBEMA's belief that if the collection of information and use of information processing techniques are given proper consideration, they will prove to be a benefit both for the individual and for society. We recognize that balance is needed to ensure protection of individual rights while at the same time not inhibiting the general benefits to society that are possible through disciplined use of modern technology. A proper balance in each of these areas is essential and achievable today.

A CALL FOR NON-PROPRIETARY SECURITY SYSTEMS

A. G. W. Biddle
Executive Director, Computer Industry Association, Encino, California 91316

When we left this auditorium last November it was evident that solutions to the problem of data privacy and security required the development of new laws, new techniques and new technology. As Dr. Davis said in her closing remarks, "The problems of settling the problems of individual privacy, namely:

> The desires of the individual to exercise control over the collection of information about himself, and
>
> The desires of the individual to exercise some measure of control over the use of information about himself, once it is collected,

are the responsibility of courts, Congress and state legislatures."

Last week, President Nixon established a special task force under Vice President Ford with responsibility to develop legislative programs addressed to these problems. In doing so, he further focused the attention of the nation on the need for privacy and security *and* escalated the need for technical safeguards for both present and future systems. It is this—the area of technology—that I would like to discuss.

The technological development of secure data processing systems represents a complex, expensive and time consuming undertaking. The problems that must be solved, as has been seen during the course of this and preceding conferences on the subject, range from the relatively simple to the almost insurmountable.

However, thanks to the work of the National Bureau of Standards, Department of Health, Education & Welfare, the National Science Foundation, AFIPS, ACM and IBM among others, a great deal of work has already been done to define the extent and complexity of the tasks ahead. One thing has already become abundantly clear—the design and implementation of secure systems will involve *and* impact every part of the typical computer system: programmers, operators, service personnel, CPU, memory peripheral and terminal hardware, operating systems and applications software as well as communication channels and links.

The development of secure systems will necessitate balancing the many tradeoffs; systems architecture, hardware design, software design, operational constraints, initial cost and ongoing operating costs. The achievement of our goal to prevent the violation of individuals rights and prevent the fraudulent use of both data and data processing systems necessitates careful and objective selection from among the many alternative solutions that *are* available.

The problem is sufficiently complex so as to require inputs from personnel with expertise in systems architecture, programming, cryptography, psychology, accounting, and a myriad of other specialties. It is clearly an undertaking that will require the commitment of a significant amount of both human and financial resources over an extended period of time. And therein lies the problem.

As I see it, there are presently two entities who could undertake this complex task—IBM and perhaps other systems manufacturers on a proprietary basis or NBS working through a voluntary industry/government cooperative program. I don't think that either of these alternatives will work.

Although IBM has the resources to do the job—they have already committed eight million dollars a year for five years to a major data security R & D effort—they indicate that only the results of the first two years worth of effort will be placed in the public domain—presumably the remaining effort will be for proprietary products and programs.

I personally think that this approach would be detrimental to the user, the public and the industry as a whole. We need to develop technical solutions that are equally applicable to all hardware and software—both present and future systems regardless of who makes them. It would be all too easy to develop security systems involving firmware, encryption and other techniques that would effectively lock out intruders and interlopers—*and* competitors. It would be relatively easy to argue that release of the design details neces-

sary to interconnect non-IBM terminals, peripherals or applications software might violate the integrity of the security system. Needless to say, reverse engineering would also be out of the question. As a consequence, I'm afraid that the catch phrase of the late '70s would become "A Secure System is a Single Source System." To avoid this, I don't think any manufacturer of systems hardware or terminals should be permitted to develop and install encryption devices or other security oriented systems that are unique to their hardware or proprietary in nature.

Rather, it seems to me that we must develop a framework for the implementation of multiple level controls—a set of locks of varying integrity to limit access to authorized individuals—to protect data in storage and during transmission and to audit the activity within the total system. The technology, hardware and software systems should be equally available to all manufacturers of data processing equipment—these are the locks. The keys should be solely in the hands of the user in the same way that you can purchase a range of combination padlocks from a variety of supplies and set the combination yourself.

I mentioned earlier that NBS is a possible focal point for the establishment of an industry wide cooperative program to develop the soltuions we need. Unfortunately, a voluntary, cooperative effort often fails unless the economic motivation of the participants is strong. For example, the Brooks Bill, which was passed in 1965, called for the voluntary development of I/O interface standards in order to increase the cost effectiveness and utilization of peripheral devices. Eight years later we are no closer to I/O standards than we were on the day the Brooks Bill was passed—for the simple reason that the typical manufacturer seeks to achieve maximum product differentiation in order to protect his market position. For this reason, I don't believe that a voluntary industry government effort will achieve the objectives sought by the user.

As an alternative, I believe that we should seriously consider the creation of a federally chartered non-profit "Super Underwriters Laboratory." Although time constraints only allow me to suggest a conceptual framework, let's see how this might solve our problem. Set up somewhat like the Financial Accounting Standards Board, the Laboratory would be funded by the government, producers and users of data processing systems. In time, an increasing portion of the funding would come from royalties and certification fees. The activities of the Laboratory would be under the direction of a seven man board of directors selected to represent a cross section of the interest groups involved. They would work solely for the laboratory and sever all ties with their respective employees.

The lab would draw qualified technical personnel from industry, government and user organizations and when appropriate augment their internal capabilities through the creation of special task forces or the letting of development contracts. It would be charged with responsibility to develop a hierarchy of security systems and devices suitable for installation on current and future systems. Appropriate certification procedures would also be required. The design of the "locks" would be standardized and available to all—hardware and software manufacturers and users alike. However, the "keys" or techniques needed to make a specific system secure would be assembled by the user following approved procedures. This might involve the selection and installation of a unique combination of read only chips in the mainframe and each terminal: it might involve the creation of algorithm or any of a number of other techniques.

The essential point is that the user would have control of the security system—not his suppliers. Since the basic design and operation of the system would be standardized, (albeit one of a family of standards) the laboratory would be able to develop certification tests to validate the level of security that does in fact exist in any given installation. Undoubtedly, such certification would probably become an essential part of the financial audit in the years ahead.

In summary, I believe that a neutral body should be charged with responsibility for developing and disseminating technological solutions to the data security problem. The laboratory, through certification, would, to a certain extent, be able to mandate compliance—just as Underwriters Laboratory does today.

There are undoubtedly problems associated with my proposed solution. Means will have to be provided to protect proprietary data supplied to the laboratory by manufacturers. A "public" hearing process might be required to allow for comment on any proposed system or standard. These problems can be solved.

In doing so, we will increase the likelihood that secure systems can be available on a timely and economic basis. It certainly represents an improvement over a dozen non-compatible, propriety solutions.

THE VIEWS OF THE ASSOCIATION OF DATA PROCESSING SERVICE ORGANIZATIONS

John B. Christiansen

Independence Computing & Software Corp., W. Collingswood, New Jersey 08107

ADAPSO, the association of Data Processing Service Organizations, is one of some 2,000 active trade associations in the United States. These trade associations provide commerical and trade information to their member companies, and also to local, state and federal governmental bodies.

ADAPSO represents 262 companies with 381 branches or a total of over 600 units. The computer industry according to the 1973 Industry report has 1,700 companies that employ 125,000 people. The gross revenues of these companies totaled 3.23 billion dollars in 1973. Because of the divergent functions performed by the services segment of the computer industry, ADAPSO is currently organized into 4 sections, and there could be more in time.

1. The first, and the original section, The Data Centers Section, is concerned with providing local representation to the member companies in their respective states.
2. The Remote Processing Services Section is especially concerned with presenting member company interests before the FCC;
3. The Software Industry Association is heavily involved in government areas with particular emphasis on procurement, on standards and on software protection;
4. The Data Facility Management Section is mainly concerned with documenting and analyzing the functions of, and inquiring into the scope of services performed by Data Facility Management Companies.

All sections provide a broad and interesting educational program for member companies and their employees.

Statement of Position

The Association of Data Processing Service Organizations, Inc., believes that individuals, as is their right, should receive every reasonable protection against the unauthorized use and distribution of personal information from data banks. ADAPSO, without agreeing that legislation is necessary at this time, agrees with the intent of most proposed legislation to date:

- Information gathered from or about an individual for one purpose should not be used for another purpose;
- Untimely or erroneous information about an individual should be subject to amendment or correction;
- There should be no personal data record keeping system whose very existence is secret.

Unfortunately, however, the bills proposed to date include wording and restrictive clauses to accomplish these commendable goals, that demonstrate an ignorance to the special economic characteristics and problems of the computer industry and especially its services segment.

ADAPSO calls on its industry to pursue an intensified effort to ensure that whatever government regulation or legislation is necessary, is undertaken only on an informed basis and with full knowledge of all the consequences.

Further, ADAPSO calls attention to the body of knowledge about the social aspects of the Privacy Problem which was gathered and published by a government-sponsored committee. The report, available at GPO book stores, is entitled, "Records, Computers and the Rights of Citizens," and has been the subject of an August 3, 1973 ADAPSO Bulletin. This report could provide the basis for establishing standards sensitive to the high rate of technological change, sensitive to the esoteric, complicated economic structure of the computer industry and its services segment, and designed to effectively protect the privacy of the individual. ADAPSO further recommends that local, state and federal agencies publicize the findings of the Committee report, and respectfully recommends all government agencies establish guidelines based on the findings of the report.

Public Should be Informed of Costs

One of the primary functions of government in a democracy is to disseminate information to its citizens, because of the widely held belief that the foundation of an effective, active, stable democratic government is an informed citizenry. However, there is currently an enormous burden on the taxpayer to support the collection and maintenance of information which is classified or whose circulation is restricted in some way. Proposed legislation regulating computer data

banks contains provisions requiring computing firms to report on the nature and use of their data to designated authorities. ADAPSO urges its industry and the government to provide the public with more information about the issues and costs involved in policing the thousands of computer systems maintaining and transmitting personal data.

Other Economic Considerations

The building and maintenance of a broadly covered, universal computerized data bank is very costly. There is a market for this kind of information, but this market must provide enough economic incentive to justify the huge on-going costs of maintenance. Because of this cost factor, it would not be possible for a commercial, computerized data bank to secretly exist that held current information about a sizeable percentage of the population. ADAPSO believes that these cost factors, along with new regulations defining ownership of personal data, would sufficiently limit proliferation of this data. On the other hand, the cost of a government bureaucracy required to protect against commercial computer data banks that target specific groups or classes of individuals would be considerable. Indeed, the size of this bureaucracy would not be restricted by the balance of costs in the marketplace, and the economic impact on the thousands of small, independent data processing service companies who would be required to feed the bureaucracy up-to-date information on their mailing lists, accounts receivable files, and the like, would be disastrous for the industry.

Efforts to Standardize Personal Data

There are government agencies urging the standardization of codes for personal identification, location, time, personal characteristics, and medical and physical status descriptors.

It is obvious that universally applied codes in these areas would aid in the accumulation and interchange of meaningful personal data, and would reduce the cost of building a data bank. However, the key code necessary to concentrate personal data from several sources is some universally accepted system of linking this coded data to an individual. The pragmatic computer systems designer will specify Social Security number as this identifier *unless* the public is aware of the dangers of the universal use of the number as a key to personal and private data. It must be apparent that the computer systems designer in industry is only following the lead of the computer systems designer in most government agencies where Social Security number has really become Federal Identification Number. ADAPSO recommends that government and industry efforts to standardize the encoding of personal data descriptors for the purpose of information interchange include the question of personal data ownership.

THE PROFESSIONAL ASPECTS OF PRIVACY AND CONFIDENTIALITY

Robert W. Rector

Executive Director, The American Federation of Information Processing Societies, Inc.
210 Summit Avenue, Montvale, New Jersey 07645

While I wholeheartedly support the need for coherent legislation, technical guidelines, and improved hardware and software mechanisms for handling privacy and security in computer systems, I submit that we are remiss if we do not take some time in a series of conferences on Privacy and Security to talk about the true role of people—not just people as "passwords," "inquirers," or "authorized personnel." I mean, in particular, the *information processing professional* and his organizations. Congressman Jack Brooks alerted us to the fact that when we deal with complex computer bases systems, no legislative action can be effective without the corresponding technological advances to support legislative efforts—and I add that no technological advance is effective without a sense of professional responsibility among the people involved.

I was surprised in reviewing the proceedings of our earlier conference that no one identified the role of the "professional" as such. Yet at that meeting almost all of the participants probably belonged to one or more professional societies in information processing or closely allied fields. I am sure that many of you here today are members of at least one of the thirteen Constituent Societies that form the American Federation of Information Processing Societies, Inc. What might be our chagrin is that this meeting is not held under our sponsorship, or that of one of our Societies, is mitigated by the thought that former conferences and workshops sponsored by the Societies have done much to stimulate and focus the interest in privacy matters that exists in government today. Probably the first serious statement of the problem, along with a suggested remedy was Paul Baran's paper *Communications, Computers and People* at the 1965 Fall Joint Computer Conference. Other landmark papers are to be found in the Proceedings of subsequent Joint Computer Conferences.

Let us then look at the role that the professional plays—as a part of the problem and as part of the solution. Certainly it is easy to demonstrate that the

professional is central to all aspects of the privacy problem.

• As a consumer—The authorized recipient of output and the supplier of input—who, in the higher echelons at least, should be concerned about what is "proper" and "useful." These customers are often members of the formal professional societies such as the American Institute of Certified Public Accountants, the American Medical Association, the American Bar Association. The fact that such user oriented societies have specialized subgroups to deal with computer based information systems is recognition of this role.

• As a producer—The systems analyst and the application programmer are the backbone of the membership in the Constituent Societies of our American Federation of Information Processing Societies.

• As a servicer—certainly in the classic sense of the systems programmer, but also in the ancillary function of operations, there is a growing association at the management level, at least, with the professional societies operating in this field.

And finally, I regret to say,

• As an intruder—The evidence already presented points out that the unauthorized entrant to data systems is not uneducated or untrained. He may be the most "professional" of the professionals. Since few of our professional societies have taken steps to act on cases of malfeasance, we may assume there are intruders in the ranks.

Surely then there is a close interaction between the professional in information processing and problems dealing with privacy and security. If we approach the problem through people—professional people—we should ask the question what are the steps that have been taken or can be taken, to solve the problems that in the end effect all of us? But first a caution: If the thesis is to promote professionalism to solve all our problems, we may be in trouble. If professionalism equates to Godliness, we may end up as zealots without solving the real problems of the world. I trust none of us will take such a cavalier attitude for there are real contributions that have been made by the professional societies in data processing. The critical question is, "Are we doing enough?"

Over simplifying the purpose of a professional society, let us describe its two major functions as protection and promotion through education. Both of the terms, protection and promotion are used broadly. They cover not only the professional himself but they refer to a number of audiences or groups and the various interfaces between these groups. I shall try to identify some of these elements with particular reference to the problems of privacy and security.

The AFIPS interest in these questions which had surfaced at all of the Joint Computer Conferences in the late sixties was brought into sharp focus with a Roundtable Meeting chaired by the Honorable Willard Wirtz in January 1970. Although it covered the larger question of "Professionalism in the Computer Field," the same concerns that bring us together today, were present then. They said, "The general public is coming to recognize that larger data bases pose threats to privacy. With large amounts of sensitive data in a data base, the competence and ethics of the persons who design and operate such systems become vital."[1]

In attacking the problem, four groups or publics were identified as requiring protection. These were (1) The "general public," (2) the "consumers of computer products and services," (3) the "employers of computer people" and (4) the "employees" themselves. In each case the degree and type of protection is different.

It is the protection of the general public welfare that provides the real motivation for our interest in privacy today. The protection of the other three groups may offer solutions to these same problems. The techniques that may be employed include the classic response mechanisms of professionals who have banded together to form the professional society. They include certification, licensing, accreditation and codes of ethics. I submit that all of these techniques can provide assistance in solving the problems that we now face.

The role of certification—an affirmation by a governmental or private organization that an individual has met certain qualifications—can be a strong influence on the field. But certification demands standards; a priori standards of knowledge and performance are necessary to attest to and maintain competence. Then there can follow the recognition and codification of "commonly accepted practice" that do much to stabilize a profession.

There are, of course, very complex problems that surround certification. The approach that is now being implemented by our professional societies is the establishment of The Institute for the Certification of Computer Professionals. This organization is investigating all aspects of the problem of certification. AFIPS for its part has developed all aspects of the problem of certification. AFIPS for its part has developed what it hopes wil be a definitive set of job descriptors and skills for the computer programmer. This is meant to be a set of meaningful descriptions of tasks and skills that will find sufficiently universal use to give rise to at least *de facto* standards. This material will be used in turn by the ICCP to study the problem of training and certification.

Simultaneously with this project AFIPS has carried on a second effort. This effort also had its genesis in the same area of certification. The concept is one of systems certification. It asserts that it might be possible to certify that a system, particularly a system in which the public had a third party interest, met the proposed specifications. In subsequent workshops the leaders came to the conclusion that it was currently impossible to define the necessary standards for systems certification and that it was difficult even to specify

[1] Professionalism in the Computer Field, 1970, AFIPS Press, 210 Summit Ave., Montvale, N.J. 07645.

preferred practices. Further discussions led AFIPS to set up a Systems Improvement Committee to explore what approaches might be taken toward developing professional solutions to the problems caused by maldesign or malfunction of computer based information systems.

To date, the committee has attempted to pinpoint questions which should be asked by any manager as he attempts to decide whether or not his systems are well designed and will perform in the desired way.

Work is now nearing completion on a manual covering privacy and security. This is the first of an intended series of Systems Review Manuals. It will be field tested and published in 1974 by AFIPS Press.

AFIPS attaches a great deal of importance to this effort. While emphasis is focused on the civil, public supported, and private systems whose maldesign could have an adverse impact on society or on individuals, the same type of critical review—pointed toward correction rather than cure—is required for all major information systems.

I believe these examples are indicative of the increased interest that professional societies have displayed in formal "Professionalism." It should also be noted that AFIPS has recently amended its Constitution to incorporate the improvement of professional standards and practices as a requirement for constituent membership. A committee headed by Donn B. Parker has been appointed to implement an active program. Some of our Constituent Societies have recently passed codes of ethics and rules of conduct. All of these actions are part of the historic pattern that a discipline must take if it expects to develop competent technical performance and ethical behavior.

Unfortunately it is not easy to fit all of information processing into the classical mold. While the essential criterion—expertise—is required, it usually has not been obtained through a prolonged period of generalized formal training and a period of practical apprenticeship or practice to perfect the accompanying skills. There is, in fact, no common curriculum, no universally accepted body of knowledge, nor any performance standards. There are compelling reasons to argue that we should never expect to reach such a steady state. The field is changing too fast! We have tapped too many other fields for talent. As a result we have ended with a young, bright, versatile, and aggressive set of individuals—all challenged by the computer and its application to the real world's problems—but somewhat prone at times to see if they could break the operating system, "just because it's there."

The other part of the challenge is the promotion of professional objectives through education. In the technical aspects, no one can fault the excellent educational job the societies have done through their publications, conferences and workshops. Their members share experience, help educate newcomers to the field and make it possible for the individual who is motivated to engage in continuing self education.

It should be noted that through these procedures, many of the mechanisms that are required for secure systems operations are already in place. If not, the hardware and software needed to do the job can easily be produced, once the specifications for security and confidentiality have been set by the public or by its authorized representatives. I believe that this is a critical question before us today—what do we want? Or rather, what does the public want? Certainly, in theory at least, the public should not oppose the collection of factual information and the efficient storage and retrieval of this information by a modern computer based system. On the other hand, the concern that follows the exposé of the abuse and exploitation of large data bases under time sharing networks should have been equally predictable. Studies have shown that every instance of computer abuse has its counterparts in an existing manual system. All of these facts pointed out deficiencies in the educational process. Anticipation of this should help bridge the interface between the consumers of computer products and the general public on one hand, and the suppliers and professionals in data processing, on the other.

What is needed is a continuing plan of education for both the general public and the professional. Professional societies should plan an educational program of bold and imaginative dimensions that will bring the challenges of data processing into true prospective. It is unfortunate that much of the interest in privacy and security comes on with negative overtones. It would be equally unfortunate, of course, if the professional did not warn the general public of the pitfalls and social costs of a proposed system.

Just as real is the need for education within the professional ranks. A recent study of programmer's attitudes shows a fantastic difference in understanding among the professionals over legal matters involving the use of the programs of others (including proprietary programs), unauthorized use of a time sharing system, and other questionable practices. Here, open discussion and education would do much to clarify the situation.

I am optimistic that these conferences on privacy and security will do much to develop understanding among professionals and the legislators. Hopefully, it will be done with the approval and understanding of the general public. If this does not happen we shall all lose.

In a larger sense I hope that the discussions that we have had here, will serve as a practicum for the professional society. What has happened in this area can happen in other types of applications of computerized systems. It behooves the professional and his society to think and act [illegible] professionals.

DATA PROCESSING MANAGEMENT ASSOCIATION STATEMENT ON PRIVACY AND SECURITY IN COMPUTER SYSTEMS

Donn W. Sanford
Executive Director, DPMA, Park Ridge, Illinois 60068

The Data Processing Management Association is the largest management-oriented professional society in the field of information processing. As managers, the more than twenty-thousand members of DPMA are very much "people-oriented," and not exclusively "technically-oriented."

As managers of data processing installations, DPMA members have perhaps a greater opportunity to see, on a day to day basis, some of the privacy and security problems which are being discussed during this Conference. DPMA members, being responsible for the implementation of whatever laws and/or regulations may eventually result from the rapidly increasing interest in protecting citizens' rights to privacy, are dedicated to finding a workable solution.

Individually and collectively, the members of the Data Processing Management Association are vitally interested, both as professionals and as individuals, in assuring that the rights of privacy of all Americans are fully and permanently protected. There is concern, however, that in the post-Watergate mood of today, that there may be those who feel that their primary mission is to emasculate what they regard as the "monster-computer."

The end result of Conferences, like this one, or future legislation and regulations, must be both practical and workable . . . safeguards which will protect without crippling business and Government. Hastily drafted procedures or laws based on fear of the "Big Brother" syndrome will surely be as onerous as the ill they seek to rectify.

In my opinion, the Bagley Bill recently introduced in the California State Assembly (as the "Computer Crime Prevention Act of 1973"), is an example of the type of "overkill" we hope can be avoided. While its purpose is laudable, and many of its provisions are highly desirable, one questions whether other requirements of the proposed Act would, in fact, defeat the entire purpose of computer utilization.

As stated by the manager of a major California County Data Processing department, the bill would "penalize organizations wishing to take advantage of the benefits of automation, thus discouraging the desirable use of computers and depriving the public of the cost savings to be realized from computerization." And, why should data stored in computers be subjected to restrictive regulations not also applied to records stored in manual systems? Shouldn't "obsolete data" be purged from file cabinets, too?

In his statement on The American Right to Privacy, President Nixon quoted from the Federalist Papers wherein James Madison declared that government has "twin duties" to "secure the public good" while "securing the citizens' "private rights." Inherent in this quotation is recognition of the need for balance between the two—neither should be regarded as more important than the other.

It is this delicate balance that DPMA feels must be kept in the forefront. We agree with the President's statement that "it is becoming much easier for record-keeping systems to affect people than for people to affect record-keeping systems" . . . and further endorse Mr. Nixon's action to seek ways to assure that people dominate the machines, rather than awakening some dark morning in an Orwelian world.

Again quoting from Mr. Nixon's February 23 address, he stated that "At no time in the past has our Government known so much about so many of its individual citizens. This new knowledge brings with it an awesome potential for harm as well as good—and an equally awesome responsibility on those who have that knowledge." I would add that not only does government know more about all of us than ever before . . . so now does the business world.

It is "the awesome responsibility" referred to by the President that most concerns DPMA. The equipment manufacturers will provide the hardware and modified architecture to protect the physical data and the computer center . . . others will focus on the design of "secure software" which will help reduce risk of unauthorized utilization of information in the computer. But let us all remember that it is the *user* who must implement the systems, comply with the safeguards, and assure that all new requirements are being met.

Both as professional data processors and as citizens, the members of the Data Processing Management Association will support a positive approach to the privacy issue. Indeed, so will the thousands of members who make up the dozens of other computer-related organizations represented here this morning. It is imperative, however, that members of all these groups—not just DPMA—get involved now in helping to draft and test the new procedures and operational concepts which will be required to make the result practical instead of foolishly idealistic.

In closing, I am happy to report that DPMA's governing body will consider at its meeting next week, a newly drafted "Standards of Ethical Professional Practice Regarding Individuals' Rights of Privacy." Recognizing that codes of practice are merely words on paper unless adhered to, we feel nonetheless that this one small step is better than none at all. These standards were drafted by Mr. Robert Marrigan, CDP,

DPMA International Vice President for Government Relations, who is attending this Conference. I would like to share these standards with all of you:

The members of the Data Processing Management Association, recognize their responsibility to:

1. Continuously strive to honor the rights to privacy of all individuals by using the information provided for their use only in the manner for which it was obtained and intended;
2. Uphold the responsibility of trust, implicit with their professional status, by maintaining the confidentiality of data entrusted to their care;
3. Avoid using information of a confidential nature to further their own personal interests;
4. Attempt to remove any misleading or inaccurate data associated with any individual, immediately upon learning that its current status is in error.

Granted, these are but words on paper . . . and in fact, have not yet been adopted. We hope, however, that they can be considered as a sort of Hippocratic Oath for Professional Data Processors who recognize their obligation to protect the citizens of this nation.

We obviously see the need for stronger more effective rules, laws and procedures, but hope that a balance will be maintained to assure what many have called the greatest business development of all time—the computer—will not be reduced to piles of rubble, unable to help because it's been rendered powerless to harm.

To quote another American President . . . "Come, let us reason together" and let computer users, technicians, government agencies, and citizen representatives all sit down calmly and cut a path through the looming morass of laws and regulations which could harm as well as help.

A SYSTEMATIC APPROACH TO DATA SECURITY

R. L. Thomas and Robert H. Courtney

IBM Corporation, Old Orchard Road, Armonk, New York 10504

Mr. Thomas

This meeting and the conference last November focus upon the need to bring additional understanding to the complex issues of privacy, confidentiality, and security, particularly as they relate to computer systems. Bob Courtney, the next speaker, and I appreciate this opportunity to discuss some of the areas in which IBM is active to help in the resolution of these problems.

As a manufacturer of computer systems we recognize our responsibility to assist our customers in achieving the data security they require. To offer systems, products, services and counsel that clearly contribute to the solution of data security problems.

Our earliest activities in the security area were prompted, frankly, more by our customers' need to secure certain business information than "privacy" motivations. Historically, customers have expressed a strong desire for broader and easier access to systems, and a relatively low level of demand for data security. Today the demand is somewhat greater and a variety of security techniques and capabilities are available to provide a level of security commensurate with the risk-cost trade-offs most desire. But the demand from customers for computer security features still ranks below other considerations such as price, performance and other special capabilities.

It is our feeling the awareness and identification of the needs of security will increase in the future, and demand for product features and systems solutions will grow considerably. And although certain tools and techniques are available today, we feel it would be wrong for the industry to wait until that demand becomes pressing before taking the necessary steps to meet the problem.

As many of you know, at the 1972 Spring Joint Computer Conference, T. Vincent Learson, then Chairman of the IBM Board committed IBM to a significant investment in the study of the requirements of data security and for further development of appropriate safeguards for IBM products. For example, the cryptographic techniques included in the cash issuing terminals of our recently announced finance communications system.

Another part of that investment has gone into a two-year joint study begun in 1972 with MIT, the State of Illinois and TRW; each giving special emphasis to a particular aspect of data security. We plan to publish the results of these study site efforts by the spring of this year. We do not expect significant technological breakthroughs; however, the results evaluate several key factors in data security protection and identify requirements for secure systems. Further, they confirm the belief, that an effective security system must include the total environment: physical and procedural safeguards as well as those provided by hardware and software. Results are based upon actual experience with the Resource Security System and include observations and recommendations relative to identification, authorization, journaling and programming system integrity. The understanding gained on data security as a result of this work will be placed in the public domain. While only some of the pressing data

security questions are answered, we believe the results will be of assistance to the entire data processing community.

Through our marketing organization we have developed a data security awareness program. It is designed to make computer users aware of potential exposures and alternatives to address them. Briefings and discussions have already been held with many companies, and industry groups, and earlier this year we increased our capability to reach even more organizations. One part of this program includes the publication of brochures on several aspects of data security. Another part was a series of data security symposia where attendees submitted papers on their data security needs and experiences. Thirteen government agencies participated to date. One symposium was specifically designed to interchange information and requirements on this vital subject with members of the auditing community.

But much more needs to be done. This is particularly true in light of the increased attention being given to the issue of "privacy."

I believe there is general agreement that technology alone cannot assure desired levels of privacy. But data security can obviously assist in assuring privacy and technological advances can improve control and reduce the threat of improper disclosure of personal or confidential data.

In this regard, IBM is pursuing programs to improve the data security capability of currently available products, particularly for complex systems environments. For example, we have placed considerable emphasis on the integrity of our OS/VS2 Release 2 System Control Program. And we have made data security a basic design criterion for future systems and products, and as we gain a clearer understanding of evolving data security needs in the marketplace, we expect to be responsive to them.

I would like to make a few brief comments at this point concerning privacy. Fundamentally, the privacy issue is not technological, and it cannot be solved by technological solutions alone or computer manufacturers alone. If society is to guard against the misuse of information about people, there must be sound public policies. The responsibility to shape prudent public policies must be shared by legislators, government agencies, computer users in government and industry, computer manufacturers and private citizens.

I believe that portion of the summary of the November 1973 NBS Conference dealing with privacy very well covers the observations made at the conference and does much to clarify a complex and often times emotional subject.

In my view, some of the observations and others deserve emphasis and consideration:

First, there has long been an inherent conflict between the interests and rights of an individual and those of government and private institutions as they relate to the protection of confidentiality of data as opposed to the desire for greater freedom of information in support of expanded services and programs at all levels. Although it is true the introduction of automated data processing has heightened this conflict and posed serious questions about precautions required to protect individual privacy, it is also true the computer can be a key factor in achieving desired implementation of privacy principles when they are defined and agreed upon.

Second, proper focus and attention of many parties must be brought to bear on the problems of privacy so as to strike a balance between the need for privacy versus the legitimate need for information, and this must include a clear consideration of the costs involved.

Third, any consensus concerning privacy principles or information practices must include input from custodians of information systems. And once arrived at, these principles and practices can provide meaningful guidelines for the development and application of the technology.

Fourth, we believe information practices as they relate to personal information must inherently embrace manual as well as automated record keeping systems, because sensitive information also exists in manual files.

Fifth, if it is determined legislation is necessary, the legislation should focus upon principles and information practices relating to personal data, and should attempt to resolve the major issues of interpretation as they may arise in practice. [I might add, the first step from a legislative viewpoint ought to be a determination of what information should be collected, by whom and to whom it may be made available.] In any event, any legislation enacted should leave ample room for the innovation of both computer users and manufacturers to provide alternative security means to achieve the intent of the law makers. Otherwise, we all run the risk of having "secure" systems which do not in fact assure privacy, plus the risk of stifling the evolution of technology.

Finally, we support Dr. Ruth Davis' comments concerning the need for a national coherence among laws defining the privacy rights of individuals and the basic information practices to be followed in protecting these rights.

In summary, the privacy issue must be dealt with through sound public policies which: reflect a balance between the need for freedom of information and need for privacy, result from the concensus of all affected parties, cover both manual and automated systems, and which will provide for a uniform approach in implementation."

Concerning data security, we are not without tools and procedures to address today's problems. But we must anticipate future needs—and we are working to provide better solutions to those problems. Bob Courtney, of our Systems Development Division, has been involved in our data security activities for six years and is known to many of you. He will discuss a systematic approach to data security.

Mr. Courtney

Among the many mistakes which I have made in this particular job one of the most embarrassing, when reviewed a few years later, was the early assumption

that the implementors of data processing systems would find it rather easy to satisfy their data security problems if the vendors simply made available to them a comprehensive array of security measures in the hardware and software products. The installation management could then shop among these items, cafeteria style, picking those things which seemed appropriate and rejecting others to the satisfaction of their particular needs. Indeed, we have recognized the provision of these security measures to be a responsibility of the vendors, but the availability of these security functions or features in the products, while often necessary to the attainment of an adequate degree of security, are not in themselves sufficient.

As we began several years ago to examine the security concerns and requirements of data processing installations, it became quite apparent that before security measures in hardware and software could be effective, much additional work was also required in the areas of physical security and operating procedures. But perhaps even more importantly, if possible, was the need for a rational, systematic approach to the identification of appropriate data security concerns, to the conduct of a workable risk assessment leading to quantitatively expressed statements of the risk involved and the impact on the organizations or enterprises dependent on the security of the data, and, finally, to the selection of security measures appropriate to these now-defined problems and their quantitatively expressed magnitude.

It is the purpose of this presentation to describe for you a structured, systematic approach to the determination of data security requirements and to their satisfaction. It is my hope that in some small way this proposed methodology will contribute to a better undersanding of the problems we are addressing here and permit easier communications between us as we seek acceptable solutions.

Communications among scientists and engineers engaged in the pursuit of some common goal are frequently, if not generally, characterized by strong differences of opinion as to how problems might best be solved and the goal achieved. The pursuit of data security is no exception. In the case of data security, however, I suggest that the widely diverse opinions are more properly attributable to differences of opinion as to the effectiveness or applicability of specific security measures to any given problem. A discussion of the effectiveness of any particular security measure can only follow a statement of the problem to which it is to be applied. The cat was right when it told Alice that it made little difference which path she took if she didn't know where she wanted to go.

It is difficult to find two data processing systems whose security needs can be effectively and economically satisfied by the same set of security measures. There is then no single data security problem. The differences are both in kind and in degree.

Data Security refers to the safety of data from all of the unfortunate things which can happen to it: that is, safety from accidental or intentional, but unauthorized, modification, destruction, or disclosure. The relative weighting of each of these on a scale of concerns will vary widely not only between EDP facilities, but usualy from file to file within a facility as well. So then must the appropriateness of specific security measures vary as a function of both their effectiveness in containing any specific concern and their cost in terms of performance burden or dollars.

If the foregoing proposition can be accepted, then it follows that a comprehensive problem statement should precede the selection of any security measures. Even partial problem statements followed by piecemeal selection of security measures are very risky because in this mode we are trapped into selecting measures which contain the partially defined problem but which may well not be broad enough in scope to contain other aspects of the problem as it may be stated once all aspects of it are fully developed. Thus piecemeal problem definition and piecemeal selection of solutions will probably crate lavering or overlapping security functions with the result that, in the end, security is achieved only at costs which are unnecessarily high. For this reason it is my suggestion that comprehensive problem definition must logically precede the selection of security measures, whether these be hardware; software or the still somewhat more familiar physical security measures.

As an example, let's consider a not very hypothetical situation in which we decide that we would like to have our back-up tapes protected in the event of an overwhelming disaster of some type, including nuclear attack. Such decisions are commonly made without much regard for the current probability of occurrence of such events. Later in some subsequent iteration of our piecemeal problem definition we find that we must also have availability or back-up files to recover from mistakes in the data processing operation which result in the destruction of the local working data set. We need the back-up files for recovery but we have stored them hours away by motor vehicle in an abandoned sale mine. It is probable that our data is seldom in greater jeopardy than when being transported on the public highways. Thus by not examining all of our needs for data for recoverability we have probably satisfied our requirements for recovery from low-probability catastrophic events but have greatly hampered our ability to recover from more mundane but higher probability catastrophes.

A convenient place to start our systematic approach to problem definition is by first listing some of the principal reasons why we should be concerned for the safety of our data. This list should then be borne in mind as we proceed through a threat analysis and risk assessment and to the selection of appropriate security measures.

I believe that the following six motives for security are appropriate to practically all data processing applications.

1. The near-total dependence of most organizations using EDP on the continued availability of the system and data. Very rarely do we have the alternative of going back to a manual mode of operation.

2. Data is a major asset. It is acquired at significant cost, it is needed to conduct the business of the organization, and it must be replaced at significant cost if lost. In these respects it doesn't differ materially from other assets which must be protected.

3. The need to protect private or proprietary information from disclosure to those who should not have it.

4. In implementing many of today's systems we worked quite hard in making the systems as easy as possible to use and in extending the services of the system to all of those who could properly use it. Unfortunately, we at times quite inadvertently provided new opportunities for dishonest people to misuse the system or data. Thus our concerns for security must extend to lessening the probability of financial reward to dishonest people.

5. This item is in some ways a corrolary of the one immediately preceding it. Fair personnel practices require that we be able to fix responsibility for dishonest activities so as to remove from suspicion all honest people who share in the programming, maintenance, operation, and use of the data processing facility. Thus we must have the ability to identify the dishonest people so as to remove all other users from suspecion.

6. The management of an installation must be in a position of demonstrating to more senior management that it has, in fact, been a responsible steward of the resources entrusted to it, that reasonable things have been done to protect against reasonably anticipatable problems.

When considering the data security issue we all have a very human tendency to postulate technologically elegant and dramatic means of intrusions into the data processing systems. We tend to resist consideration of the mundane and unexciting if for no other reason than it appears to afford little intellectual challenge. However, I propose to you that the solution to the mundane problems is more intellectually challenging than are the solutions to the more dramatic situations. Now to proceed in an orderly fashion through our look at security requirements, I propose that we next take an utterly pragmatic look at the security problems we actually encounter.

If we list in order of decreasing probability, that is most probable first, the unfortunate things which happen to systems and data, we find at the top of the list, leading all other items by a very significant margin, the all-too-familiar problem of errors and omissions.

Dishonest *employees* are send on our list. It is important to note that most of the data available today on fraud and embezzlement involving data processing systems reveal that there are very few instances of significant loss in which an employee was not involved either alone or in collusion with others outside the organization. These same data also show that employees tend to use dishonestly those data and system functions which they have been authorized to use in order to perform their jobs. In general, dishonest people working in accounts payable manipulate accounts payable and inventory control clerks manipulate, to their own advantage, inventory files. Inventory control clerks do not manipulate payroll and payroll clerks do not modify accounts payable files. People tend to use dishonestly those capabilities which they have been given and with which they have developed detailed familiarity and, apparently, contempt. They are not inclined to cross functional barriers within the organization. They perceive less risk of detection within, rather than beyond, their appointed domains.

Third on our priority list is fire. A fire does not have to be in the machine room to completely cripple the data processing operation. Fire which denies the data processing system power, or air conditioning or even access to preprinted paper forms on which the system is dependent can be completely crippling. It is apparently easy to forget this. When planning fire detection and fire quenching systems for the EDP room we rather frequently forget that we need a similar capability in the areas immediately adjacent to it, which quite often have larger quantities of combustibles in them than do the machine rooms themselves. The last fire we had start in a computer was a Model 650 in 1957. Thus, this is not a high-probability source of fire. The last operation which was crippled by fire starting elsewhere was much more recent.

Fourth on the priority list is disgruntled employees. The amount of damage done in this way, is relatively small, but the per incident impact is sufficiently large to warrant concern. Problems in this area which have resulted in significant dollar loss seem for the most part to have either been easily avoidable with accepted management practices or resulted in greater loss than necessary becaus problems continued far too long as a result of insensitivity to pain on the part of the installation management.

Fifth, we have damage from water. Floods and natural disasters are of course a problem but I suggest that stockholders, depositors, policy holders and voters are much more tolerant of losses to major natural catastrophes than they are to readily avoidable losses due to a leak in the roof or defective plumbing on floors above. A significant percentage of the losses due to water are readily avoidable with a modest investment in a roll of polyethylene film and a pair of scissors. This modest investment, in the order of $15, can avoid major water loss.

Finally, in last place, accounting for a very small percentage of the losses, but not to be ignored of course, is the loss due to "others." These are the losses attributable to people who have no current or immediate past involvement with the system, who are in effect strangers penetrating our systems. Mr. Robert Abbott of the Lawrence Radiation Laboratory noted in his talk at the 1973 session on Controlled Accessibility at NBS that he had been unable to identify significant losses due to technologically complex intrusions into data

processing systems. Our findings fully support his. We have seen attempts and we have seen minor losses but we have also seen numerous instances in which attempts were made primarily because of the intrinsically interesting technical challenge but during which the intruders either would not or could not exercise their intrusion in such a way as to do significant damage.

In prioritizing the probable exposures of any data processing installation to loss of data security there is a very natural, human tendency to consider things which might happen but which have never been known to happen, which have a low probability of occurrence and the avoidance of which might impose considerable cost or inconvenience on the data processing facility. We can always imagine a much wider array of malicious activities on the part of people than we can reasonably anticipate happening. Rarely will we be able to afford to protect ourselves against everything which might happen. We must reserve our concerns for those things which happen with a sufficiently high probability to justify corrective measures including, where appropriate, recovery rather than avoidance. Hypochondria is itself an illness.

The next step in our examination of our security needs, after threat analysis, is risk assessment. A detailed explanation of the approach which we have developed is well beyond the scope of this presentation. However it involves an examination of each of our important data aggregations in the light of the six bad things which can happen to these data, so as to determine the possible dollar impact of each thing happening to those data and a gross assessment of the probability of occurrence so as to arrive at a statement of risk in cost per unit time, such as dollars per year. I will be glad to discuss this technique at some later time with anyone who is interested.

This leads us to a discussion of the selection of specific security measures. Before going further into this though, there is a point which I would like to make with some emphasis; that is, that in putting security measures in our hardware and software we have not attempted, or even thought it advisable, to introduce security measures now which may be needed in the future but for which no significant number of people have current need. Our efforts have been to introduce security measures appropriate to the needs of the time frame in which the particular product will exist. There is no more justification for unwanted or unneeded security measures than there is for unneeded functional attributes of any other kind.

Security measures fall into four distinct categories. These are identification, authorization, audit, and system integrity.

If we wish to selectively constrain people to doing only those things we want them to do and deny them the opportunity to do things we do not want them to do, then we must be able to uniquely identify these people. Similarly, we cannot hold people individually accountable for actions they have taken on the system unless we can compile a journal in which the individuals are uniquely identified and associated with these actions.

All schemes for the identification of people to the data processing system fall into three basic classes. We can use something you know, such as a password; something you are such as a voice print or finger print; or something you have, such as a badge or credit card.

Of the three basic means for identifying people the one which has been used most for identifying people remote from the system at terminals has been something you know, such as a password. Passwords are inexpensive to use but passwords are also very weak. People have a strong inclination to give the password to anyone with whom they work who can help them do their job as a consequence of having that password. The security of the password scheme is difficult to audit because people who have just given away their password or people who have received it look no different as a consequence of having done either. Attempts to improve on passwords through the so-called extended handshaking, that is through the use of questions which presumably only the right person knows the answer to, have only occasionally been successful and then only in applications where the sessions are long and not too numerous. Then, only, does the time spent in discussing identification with the system not constitute a significant performance burden.

Another class of schemes for identifying people is to examine the completely personal parameters which are unique to the individual. This of course has been the way in which we have classically recognized people all of our lives, that is by looking at them and seeing who they are. Personal recognition, including the use of picture badges is of course a frequently acceptable way of identifying people who are bringing work to the window of a batch shop. Its principal failing is not in the identification area but in the failure of the person receiving the work to check the authorization of the recognized individual to do what he has asked to do, to run the job submitted.

The use of personal parameters for the identification of people at remote terminals provides some interesting challenges. Fingerprints occur almost automatically to anyone who considers this problem. Our current assessment is that, while fingerprints have great value in verification of personal identification in the law enforcement environment, they do not appear to be well-suited as a low cost means of identifying terminal operators to a system. The cost of reading in the fingerprint, the amount of data which must be transmitted to the device which does the identification and the need for rotation and translation of these data before interpretation all appear to make the technique economically, if not technically, infeasible in the near future. Speaker verification through analysis of pre-stored voice patterns is technically feasible but contributes significant technical problems in practicable implementations. Noise on common-carrier lines, variation in microphones and the need to transmit voice and digital data over the same lines and segregate them on the receiving end all serve to significantly complicate the use of this technology for operator identification. We did conduct a rather extensive test of this technology on several dozen terminals at our Advanced

Administrative System (AAS) and then discontinued its use because of these complications. We have other technologies in this category which we are currently pursuing but with no strong indication of their probability of success at this point.

In the last category of identification schemes is something you have, that is the badge or credit card. In recent years we have introduced magnetic stripe credit card readers on some terminals on which their use appears appropriate. This seems a solid, readily workable technique for identifying the operators of those terminals to the central system. Added security can be achieved through use of these magnetic stripe credit cards in conjunction with a password or employee number or name if these are not embossed on the card — and they should not be.

There is a need to avoid loss of private or proprietary information through inadvertent transposition of terminals during transactions. To this end, we have built into all of our newer terminals, which may be connected to a system through the switched network, factory-assigned, hardware-generated terminal identification characters. In addition, we have added to our transmission control units appropriate circuitry to permit program sensing of loss of continuity of connection so as to indicate the need to check the identification of the terminal before transmitting data to it.

In some applications it may be desired to check the authorization of the terminal, as well as its operator, to access the data or perform the transaction solicited from the terminal. The hardware-generated characters can also be used for this function. In general, however, terminal identification hardware has its greatest value in preventing inadvertent loss of data. It is not overly difficult to build an imposter terminal so this technique does not lend itself to protection against technically competent, malicious people who would intrude through impostor terminals. It is certainly no substitute for good operator identification techniques.

We have previously defined authorization and audit as primarily the functions of constraining people to those things we want them to do and to keeping a record of what they, in fact, did. Somewhat earlier we also noted that people seem little inclined to attempt intrusions into portions of the system to which they are not normally authorized access. If, however, it is possible to increase the difficulty with which they can do this, and at a cost commensurate with its value, then it should of course be done. However, of the two functions, authorization and audit, the journalling of what people have done is usually, if not always, more important to the achievement of security.

We have extensive experience in the application of both authorization and extensive journalling in our own internal Advanced Administrative System. Each system user is quite effectively constrained to only those functions which we wish him to perform and to only those data which he needs to perform those functions. In addition, we do extensive journalling so that we can extend to our 7000 authorized users on 1100 terminals the assurance that, if they do what they have been told not to, there is a high probability that it will become known. Although much of the data within that system is sensitive and of great importance to the successful operation of our business, we believe our data to be far more than adequately safe and that we are completely justified in our continued dependence on its security there.

The previous speaker, Mr. Thomas, referred to the Joint Study activities and the planned publication of the results of these studies. Included in the work done at the Joint Study sites was a detailed examination of the requirements for authorization in future systems. You should find the description of that work interesting and informative when it becomes available.

The fourth category into which we classify our security measures is system integrity. This includes the proper functioning of hardware, programs, appropriate physical security and operating procedures and the required degree of safety against eavesdropping and wiretapping. After several years of reviewing functional objectives for new products, the functional specifications and actual designs, I have been forced, quite reluctantly, to the conclusion that, while general guidelines for the design of hardware to eliminate potential data security problems. The number of ways in which people can inadvertently introduce data security problems exceeds by far the ability of any author of a design guide to conceive priori all of the ways in which such problems might occur. Thus we have found it desirable to maintain the function of critically evaluating each new product for potential data security problems so that we can correct that design prior to completion of the development process. As a result of this activity we have specificaly modified the design of numerous devices to improve the safety of data as it might be affected by that device.

Many of you are aware of our announcement of OS/VS2 Release 2 as our high-integrity system control program. For reasons which everyone here, I am sure, appreciates, we did not announce this as a "secure" control program. We did announce that we had corrected all integrity deficiencies which we have been able to identify and committed to the correction of any others which are identified for us. An extensive effort was made to identify all potential deficiencies and, as a result, we believe that if any remain they will be difficult for an intruder to exercise. We hope that will be the case.

I will not speak further to the requirement for physical security and operating procedures.

In the matter of eavesdropping; that is, intercepting emanations from the system, it appears now technically infeasible for eavesdroppers to acquire information from a CPU of more than very modest size and its immediately attached peripheral devices. For this reason, and because of their extreme cost, we have seen a steady decline in the use of screen rooms about centralized data processing facilities.

There is reason for concern for the susceptibility of terminals, including any small, remotely-located, serial-by-bit devices for the loss of information to an eavesdropper. We have no indication whatever of any loss of data in this manner. However, if it is known or

believed that the data in the system is of very high value to others, then a degree of concern is justified.

It can be shown that the cost of intercept to the intruder as a function of his distance from the device is generally a very steep curve. His costs increase dramatically as he is forced away from the emanating device through control of the immediate surroundings. It is our belief, based on rather extensive experience in this area, that it is economically infeasible to attempt to build devices which have such a low level of emanation that no further concern for the eavesdropper is any way justified. The cost of this low emanation characteristic heavily impacts the cost of the device.

As an alternative we have decided to evaluate each new device offering a potential for this problem so as to determine the probable cost/distance relationships to be encountered by the eavesdropper so that we can offer our customers guidance in the selection and placement of terminals and in determining the amount of geography over which they should maintain surveillance to make improbable the loss of data in this manner. If anyone has a concern in this area, we will be glad to discuss it with him and offer appropriate guidance.

Now to the last item in our system integrity list—cryptography. We will not discuss here the particular algorithms which we have developed. I would however, refer you to the lead article in the May 1973 Scientific American for a highly readable dissertation on that subject by Mr. Horst Feistel of our Research facility in Yorktown, N.Y. I am certain you will find that paper quite interesting and far more understandable than any dissertation I might offer on that subject here today.

I am certain that we can agree that the only generally applicable solution to a wiretapping problem is to encode the data in transmission. To that end we developed algorithms which we believe to be peculiarly useful in the data processing environment. We have started introducing cryptography in those products which, by their nature, invite wiretapping. Again, we are not aware of any loss of data from any EDP system through wiretapping. We can anticipate problems in this area when other ways of achieving the same results are not available and when wiretapping becomes the most feasible means of achieving the results and the rewards are sufficiently great to justify it. We believe this to be the case with on-line cash issuing terminals. For this reason we introduced the first large scale use of cryptography in the data processing business with the 2984 and 3614 Cash Issuing Terminals in which communication between the cash issuing terminals and the host CPU is encrypted.

This brings me to the end of this discussion of one possible approach to a better understanding of the data security problems. As we work to enhance both our understanding of the problem and our ability to control any problems which exist in the data security area, I am quite certain that you share with me, as professionals in an exciting business, an intense desire that our increasingly powerful systems be powerfully used and not powerfully misused.

SECURITY IN COMPUTER NETWORKS

Peter S. Browne
General Electric Information Services Business Division
7735 Old Georgetown Road, Bethesda, Maryland 20014

It is clear that we are now entering into an era of distributed computing via networks. The highly successful concepts which were pioneered by the Advanced Research Projects Agency (ARPA) network and the General Electric Time-Sharing Network have now become very well known. These concepts contemplate batch or interactive processing, accomplished remotely with output being distributed to perhaps other locations. The data base may well reside in several places. As you know, such systems are very complex, requiring an immense amount of processing logic just to handle the message protocol.

Also, 1974 is the year of revolution for computer communications. The specialized common carriers are now getting their systems in full operation. Datran and MCI are realities. Two new entries in the market place, Packet Communications, Inc. and Telenet are causing quite a stir. Therefore, the continuing trend toward marriage of the computer industry and the communications industry is inevitable.

The winners, of course, have to be the users of computing power. It will be possible to hook into a network at any time; to process against remote data bases; to tie in-house computers to those of foreign governments or companies; to query remote subsets of operations; to feed data to other remote points. Yet networking will allow, and even encourage the use of "local" computing power to do those things that are purely local in nature. The development of networking technology, with a consequent rapid growth in on-line applications, expanded the role of computers well beyond the simple functions they were initially assigned.

It is very easy to get enthusiastic about the possibilities of net working and remote computing. The effect is the same whether the network is a "star" type such as GE's with centralized processing capability at one end of a world-wide communications network, or the "topological" type, in which processing is accomplished at the various nodes. Costs are going down, and use is expanding almost exponentially.

While it may have been possible to remain complacent about security and privacy of data in the bygone days of stand-alone, in-house dedicated systems and batch processing, today, institutions are putting increasingly sensitive data into syms that can be accessed from a host of geographically dispersed locations. The November 1973 meetings here at NBS focused on the need to develop mechanisms for security and privacy in computer systems. One recurring theme was that today's systems aren't designed with security in mind, and that technical solutions are yet to come. This is only partially true on both counts. There is no doubt that the needs for proper protection have not been sufficiently addressed by either manufacturers of hardware or users of systems. It is also true that networking represents a greater threat to security than a simpler type of dedicated system. However, I hope to show you that an adequate level of security is possible, today. To achieve it requires far more attention to the subject than most people have been willing to give. We will propose some possible safeguards and solutions to problems of security and privacy, and then devise some principles to consider when designing a system or submitting a request for proposal.

Is Network Security Possible?

The increased exposure to threats faced by on-line, remote computer networking was covered very well in the November NBS Conference. In essence, remote entry allows a would-be intruder the mask of anonymity, and communications lines themselves are vulnerable to capture, passive infiltration or the problems of misroute, transmission error, etc. Jerry Hammett of Ohio summed up the conventional wisdom of the day when he stated that "interactive processing threatens security." It is true that if one looks at the vulnerabilities of a dedicated, batch oriented system and compares a remote access, time-shared, networked system, the difference in exposure is probably that of one order of magnitude greater. The following list exemplifies the additional leakage that accrues uniquely to remote computing.

1. Physical access to the computer cannot be isolated to the environs of a machine room. Multitudes of users will be accessing the central system(s) from all over the world. If dial-up lines are used, there can be no assurance that the remote location will have any semblance of physical security.

2. The communications lines themselves are vulnerable to tapping or passive monitoring of emanations. Crosstalk between communications lines or within the switching centrals can present a vulnerability.

3. Any secure system is based on the concept of isolating any one individual from all elements of the system to which he has no need for access. Normally, this is done by denying physical access to those without "clearance." In a networked system, a large population of users with varying needs to know, will be interacting simultansously with the system. This places a heavy burden on the overall security mechanisms to control the spread of information, or its misrouting to the wrong user.

4. The complexity vulnerability has already been mentioned. The more extensive the network, the greater the probability of system error and vulnerability to rational intrusion.

5. Another problem also refers to size and scope. It is virtually impossible to verify that any large software system is completely free of errors and anomalies. Also, the state of design is such that frequent changes to the system can be expected. Errors, compounded by frequent changes, can cause frightful security problems when multiplied over a large network, in which there are multitudes of large systems, all interconnected and reliant on another large system (the interfacing processors and communications protocol) to tie them all together.

The obvious question is that with so much going against it, is there really any hope for adequate protection in such systems? As we shall explore, there is some hope not only in the future, but even now, with today's systems. Much of the hope depends on what the user or owner can do on his own.

The first step toward achieving any kind of security in a resource shared system is to apply those principles of protection that would be normally put in a local, batch, stand-alone system. If the basic principles of physical and administrative security, as well as adequate audit trails and backup are followed, then the necessary groundwork will have been laid for implementation of protection throughout the network. It is imperative, however, that each location submit to the rudimentary standards of security. Such standards must be a top management concern, because nothing will defeat a security program faster than to have an independent and recalcitrant appendage off in the boondocks thumbing his nose at all the controls floating down from above.

There are many protective measures that surveyors of networks can install into their system software and hardware, to help enhance the possibility of achieving security. The next section will explain some of the measures already existing in commercially available systems.

Current knowledge about protection technology is already at a pretty sophisticated level. People like Bob Abbott of Lawerance Radiation Labs, Clark Weissman of SDC, Hilda Faust of NSA, Butler Lampson of XDS, Larry Robert ex of ARPA and Roger Schell of the Air Force know their way around the gut technical issues of the day. They know how to design secure operating systems or secure computer/communication architecture. The development cycle is already under way. At least two major mainframe manufacturers have heavy commitments in system security design efforts. I firmly believe that within one to three years we will see com-

mercially available secure systems that go a long way toward providing the kind of environment in which data can be kept totally private, even in a vast, resource-sharing network.

Finally, there is some good rationale for making the statement that networks can be inherently more secure than the more traditional kind of system. The reasons are as follows:

1. Fewer people are actually handling data. Consider the picture of a large batch system with the need for a Job Control Language Facility, Input/Output section, job scheduling, submission of jobs to the system by operators, collection of output and delivery to the customer. Then contrast this with a job submitted through a remote terminal, with its nature and purpose unknown by the network operators, who only hang tapes or disks with unobstrusive serial numbers and pass output to stations, not people.

2. It is easier to develop authorization schemes for people from terminals, where what they know (password-s) or what they possess (identification cards) can be used as the basis for system identification and authorization rather than a job control card entry which is easily replaced or forged. The anonomity of a remote location can be used to good security advantage in that all jobs must go through a pre-defined authorization process before alowed to use the computer resources.

3. The very protocol which is so necessary to even allow packets of information to be transmitted computer to computer or remote terminal to computer can serve as a security check. Additional authorization or identification checks can be built into the software. In addition, most networks utilize remote concentrators or interface message processors which have processing and memory capability. These offer a powerful tool to aid the processing, checking and auditing of security related information.

4. Many existing networks, contrary to popular belief, were designed from the beginning with security in mind. Their existence would have been very fragile any other way. Many service firms are not selling hardware; they are selling simultaneous and multiple access to central systems. And they would not stay in business very long if they couldn't protect the privacy and integrity of their customer's files and programs. There is a second reason for attention to security needs. Not only does the multiplicity of their customers make data security necessary, but they also make it possible. A broad customer base allows the heavy investment in security programs and procedures that are that necessary first step.

5. By their very nature, computer networks are targets for penetrators, whether they be actually intent on damage, whether they penetrate because the network is "there," or whether they penetrate upon invitation by the network. The net result of such penetration activity is usually to close loopholes. Our own GE Time-Sharing Network has been under attack for many years. We have hired a noted consultant to try and break its security, and he has failed to do so, even though he has been quite successful against a number of advanced DOD and Intelligence community "secure" systems. We have also never had to pay off on a $5,000 internal reward to GE employees. This is one network ssytem that is secure enough to hold the personal, private data of hundreds of organizations, each of which has an in-house computer system, but wouldn't entrust the most sensitive processing; the truly competitive and proprietary information, to its own data processing facility.

Achieving Security in Network Systems

Basic Physical and Data Security—How can such a level of security be achieved? There is one necessary condition. That is that the owners and users of the network follow some simple, yet definitive guidelines in regard to physical security, procedural security, backup and audit. These are necessary, but not sufficient conditions for any computer system, but are especialy important given the increased vulnerabilities of resource sharing networks.

Physical security standards should include very strict access control to the central elements of the network; the processing systems. Facilities should be protected from exposure to fire, flooding and natural elements, by means of construction, proper drainage, protected location, fire/smoke detection, suppression equipment, etc. The systems should be protected against utility unreliability by power source backup, uninterruptible power systems (UPS) and redundant air conditioning equipment. Good housekeeping should be not only required, but demanded.

Procedural protection can take many forms, to include the mechanics of how access is granted. In fact, this is one of the least understood and underestimated costs of security. In order to make protection work, detialed attention needs to be given to maintenance of system access rosters, followup of security incidents, self-inspections, updating of security policy and procedures and training in security procedures. In every organization I know of, this is a full time job, yet very rarely is it handled by a full time person. Most security breaks down at this level; there is no one to handle the responsibility, and things don't get done. Every computer needs a Systems Security Officer, and the higher he is in the organization, the better.

The need to provide backup for systems, devices and data is self evident. As important as the backup itself is the set of procedures or rules to utilize it. Complex disaster recovery plans will do no good, if on the evening of a real catastrophe, the plan is locked in desk drawer in the middle of the fire with no one to remember what it was all about.

The ideal security situation is to have all data movement recorded. This is impossible with today's hardware/software, so the next best step is to consider the needs for audit trails throughout the organization. Attention to the basic principles of separation of duties and accountability for actions will at least lead to possibilities of system auditability. Much of the computer abuse that Donn Parker talks about could be avoided with even simple, rudimentary attention to audit details such as internal controls for validity checks, error handling procedures, control totals, accounting for computer time and spot verification of computer output. The internal auditor needs to play a large role in the data processing part of the agency or business. He should not only evaluate existing controls, but should recommend new ones and should be consulted in the design phase of any programming project.

All of these points are brought out very forcibly in the new NBS publication "Guidelines for Physical Security of Automatic Data Processing Facilities." It is highly recommended. It will help any agency provide that necessary first step in achieving system security.

Systems Security (Controlled Accesssability)—True network security can only be achieved today through modifications to systems software and/or hardware. As mentioned by other speakers, today's commercial systems don't have the necessary modifications. There are some systems, however, that are achieving an adequate level of security. Notable is the GE Network, as well as efforts by the Air Force to develop a truly certificable versions of the Multics System. Intelligence processing networks have achieved better security than many non-DOD systems need. The principles of design that distinguish these networks from the more mundane variety have been or will be covered by other speakers in this conference. A review of some basic principles would be in order, however.

First of all, access to the system must be rigidly controlled and enforced. This implies that the identification mechanism be one in which ambiguity is minimized and which can account for impersonations. Authentication words or techniques must be protected at the highest system level and must be changed regularly. Ideally, passwords should be random and non-mnemonic. Passwords and authetication information should be stored in protected storage, not accessible through the terminal. The terminal should be a part of the access mechanism, so that certain data/programming can be restricted from certain terminals.

Secondly, each user and process must be isolated from all other programs in the system. Hardware boundary registers, software address traps and various system states should be present.

Assembly language programming should be absolutely prohibited. All requests for data access should pass through a systems routine which mediates address requests and passes them to the supervisor as a call. This is where the inherent security of Multics or VS–2 achieves high marks for security. In addition, core and peripheral shortage should be purged or zeroed out so that there is no danger of another program or user reading the residue.

Passwords or lockwords should be assignable at least to the file level. In addition, authority for other users to access, read, write or execute private files must be expressly granted, otherwise, data is not readable by other than the "owner."

Certain groups or "cliques" should be able to further restrict access by controlling the granting of passwords and privileges, without the knowledge of systems personnel. This ability should also extend to further constrain any individual by restricting the precise programs, data files and system capabilities to which he may have access.

The adequately secured network will provide for data encryption, at least at the file level. This ensures that data as it resides in system files, on tape or on disc is secure against capture at that level.

The crucial issue in networking is the capability to encrypt data for transmission. It is a welcome sight to see the technology for encryption now entering the public domain. The advent of specialized hardware cryptographic units to interface between computers and terminals or other computers has been long needed. Their cost is presently high, but their use is growing.

Fortunately, there is hope that relatively inexpensive cryptographic transformations can be affected by modifications to terminals.

The final issue in network security is that of the transmitted packets or messages. In a star system, in which remote concentrators are used to collect, enhance and forward messages, the issue is simpler than in a distributed network, with a greater variety of routing and distribution choices. In either case the requirements are similar; to put enough routing, control and authorization information in the message protocol so that the interfacing hardware can make appropriate decisions. These decisions should be as much a part of the line discipline as the decisions regarding acknowledgement/no acknowledgement, vertical or horizontal redundancy checks and other message switching requirements.

The main points to make in regard to these measures are twofold. First of all, all the measures mentioned are available now, without having to wait for an uncertain implementation. Secondly, though implementation of all of them may not be possible, depending on the particular network in question, enough can be implemented to produce a worthwhile amount of security. It is important to emphasize that implementation of the complete set or a viable sub-set will *not* produce the perfectly secure computer network that can now magically begin to process the most sensitive and private data in the world. That utopia (or hell) probably will never come. There is no such thing as 100% security. With efforts currently under way, it may be possible to measure that less than 100%, and derive some useful quantification of what a system will protect against, and at what level. That is what we are all striving for. Therefore, to take a doomsday approach and claim that security is impossible to attain is as short sighted as to ignore the very real problems of network vulnerability. Good security is possible, today. But there are some very important conditions, most of them involving human and sociological issues, not technical ones.

Prescription

The custodians of data banks and the owners of data, as well as users and subjects, should have a large voice in determining what safeguards are present. This session, and the previous one last November addressed the question of legislation. As a concerned professional and private citizen, I welcome legislation in this area. Dr. Willis Ware's report to the Secretary, Health, Education and Welfare presented a reasoned exposition of legislative needs. Beyond this step, I believe there are two very important actions that need to be addressed by you, me and other concerned people on a national basis. If action is started now, we should go a long way toward insuring that systems are designed with security in mind and that they are capable of safeguarding individual and corporate rights of confidentiality that are so urgently needed.

Management and Operating Guidelines—Every data processing data communications environment is sufficiently different in scope, breath, purpose and size so as to make rigid rules of security very difficult to enforce. However, there are sufficient guidelines and practices that have stood the test of time. Some common standards of physical, procedural, backup and audit security can be maintained. Therefore, the first step would seem to publish and use guidelines for security, and then audit their application. NBS is bringing out such guidelines very soon. They are not written or intended to be rigid expositions of do's or don't's; rather they urge ADP installations to take a risk management approach toward evaluating the threats to data, and present ways to help reduce those threats. I urge that these guidelines become standard reading throughout the Federal, State and Local DP community, and that they be updated and revised periodically as needed. If systems ever are to become certifiable, such guidelines provide a base. In any event, they provide a starting point for audits, both internally and by GSA or other interested agencies.

Specifications for RFP's—To date, very few Requests for Proposal have included definitive requirements for security and integrity. Certainly, if we as users don't care about the subject, it becomes very difficult for the manufacturers to include it in the design of their systems. If we do care about the subject, it is about time we put our money where our mouth is. Therefore, in a spirit of User's Lib, I am presenting an outline of a model set of specifications for requesting secure computer services or systems:

1. The compufer and communications hardware should come equipped with basic security capabilities. They should include at least the following:
    a. Two modes . . . privileged and user (or master/slave).
    b. Boundary control registers, permission registers, memory protect keys or a base addressing scheme for core limits protection.
    c. Positive hardware identification of terminals and peripherals.
2. Security objects such as individuals, terminals, programs, and data must be explicitly identified to the system. For individuals, the following approaches may be used:
    a. Passwords—and/or account numbers.
    b. Credit cards, badges, magnetically inscribed objects.
    c. Identification based on personal characteristics such as voiceprint or fingerprints.

    Further authentification may be made by use of passwords or challenge and reply procedures. If passwords are used, they should:
    a. Be randomly generated and of sufficient length to avoid compromise.
    b. Be changed periodically, preferably every time used.
    c. Be protected at least in accordance with the level of data they safeguard.

    The access control system should be sufficiently flexible to support a variety of constraints and mixes of objects. Users could be checked against terminals, programs, or data. An access list could be attached to any or all of the above depending on the needs of a particular installation. Every access to a given file or device must be capable of being trapped through the access control system in order to give the capability for additional authorization or identification checks. In addition, code words (lock words) should be placed within files to prevent reading of sensitive information.
3. The security system should support separate identification for individual users, terminal stations by location, individual programs or jobs by name and function and data to at least the file level.
4. All unauthorized access and I/O requests must result in termination of job, sounding of an alarm, purging of queues and refusal of service to the offending terminal/station. A maximum of three invalid log-ons or requests for information must be alowed before a given process is terminated.
5. A journal or accounting log must be used to capture information related to log-ons, terminal/user identification, data requested, files accessed, data created and security violations. This raw data can then be formatted by user written programs to produce meaningful reports.

These specs won't guarantee security, but they provide a useful departure point. They also provide a very small subset of what is required. The main point is that they address some of the real needs of contemporary systems.

Conclusion

Achieving security in computer networks is a greater challenge than achieving it in stand-alone systems. In either case, the exercise may be like chasing one's own tail. However, we have looked at home reasons why achieving an adequate level of security in ntworks is possible, even with today's technology. The necessary, but not sufficient conditions are minimum standards of physical, procedural, backup security and audit. Postulated were a number of possibilities for enhancing system security, most of them available in current networks. There are many challenges yet to face you as users of network services. Some possibilities have been covered earlier. If you do nothing else after this session, do the following:

1. Plan for networks; they are the wave of the future.
2. Write security into the specifications and RFP's for computer services and equipment.
3. Install controls in systems from the very beginning.
4. Continually assess and audit those controls.

If these actions are accomplished, the goal of simple, isolatable, mediatable, measurable and flexible security controls will be very much a current possibility.

COMPUTER SYSTEM ARCHITECTURE AND ACCESS CONTROLS

Oliver R. Smoot

Computer and Business Equipment Manufacturers Association
1828 L Street, N.W., Washington, D.C. 20037

This morning we heard about the current and proposed statutory environment in which systems dealing with information on individuals will have to operate; and just a few minutes ago, we heard the viewpoints of the computer manufacturer and the computer professional. Now we'll begin to deal with the technical aspects of fulfilling some of these requirements set out this morning and in November.

In this first section we will continue this format of discussing what exists today and then dealing with the technology needed to respond to new requirements. The first two papers this afternoon will concentrate on two of the most important issues raised at the November conference, the first on protection of data from observation through encryption and the second on control of access to systems resources. Our last two papers present important contrasts between the concept of the architecture of self-protecting computer systems and then management's role in implementing security regardless of the hardware base.

SECURITY ARCHITECTURE USING ENCRYPTION

Richard R. Keys and Eric H. Clamons

Honeywell Corporation, Phoenix, Arizona 85005

Encryption has been extremely successful in preserving the security of private message traffic. So, why not use it for preserving the security of information contained in computers? This appears to be a good idea, but several questions must be answered:

- In which parts of a computer system can encryption and decryption be performed?
- What protection improvements will encryption provide? What are its limitations?
- Is there a cost/performance penalty to be paid for the introduction of encryption techniques?

Encryption by itself has not been found sufficient to protect a system, but when made part of a secure environment it can increase protection without causing severe economic impact.

Data in Motion

When we think of encryption, most of us think of coded messages—transmission of written information, and more recently, transmission of data by electronic means from one location to another. Messages are coded in order to protect against unauthorized interception such as monitoring of radio transmissions and

tapping of land lines. For this reason, techniques for encoding messages, particularly for classified military and other government classified communications have been developed.

As a result, a variety of electronic encryption/decryption devices are now manufactured. Secure communications are maintained through a pair of such devices by placing one encryption device at each end of the communications link. The data to be transmitted is fed into the first device where it is encoded and sent across the link; the second device receives the message, decodes it and outlines the data in its original form.

These devices can be designed so that each one can either encode or decode, allowing two-way communications. They can be designed so that the code can be selected from among many by means of a key. By periodically changing the keys in the two devices the degree of security can be enhanced.

Data at Rest

As contrasted to data in motion, data at rest is data in a semipermanent file—data on magnetic tape, data on Magnetic Disk, or even data in main storage.

The amount of encryption that can be performed depends, of course, on the cost and performance of the encryption devices available. For the moment we will assume the existence of an encryption device having no cost and having no performance limitations. Later, we will consider cost and performance constraints.

Protection of Media

The most obvious way of providing encryption on a tape or disk is to install an encryption device on each tape or disk drive in line with the data path to the recording head (fig. 1A). With everything on the tape or disk in code, the tape or disk is protected in case it is stolen, and it is easier to dispose of when it is no longer needed.

This configuration has the disadvantage that a large number of encryption devices are required. This number can be reduced by placing the encryption devices in the peripheral control units instead of in each tape or disk drive (fig. 1B). For this configuration the encryption device must be designed to be set, enabled, or disabled by the peripheral control unit. Fortunately, transfers in a peripheral control unit are tagged as data or control. This permits encoding of data which is to be recorded by a peripheral device, while not encoding peripheral control and status information. But this configuration does not achieve exactly the same results as in figure 1A. On magnetic disks, the record identifier adn key fields cannot be encrypted because they must be interpreted by the device during search operations. For many applicaitons, this may be acceptable since the data itself is still encrypted.

The encryption device can also be placed in the input/output controller (fig. 1C), but now the encryption device must be enabled or disabled not only according to whether control, status, or data is being transmitted, but according to which peripheral is receiving the transfer. Transfers should not be encrypted for unit record devices such as the line printer, console, card reader, or some of the tape or disk drives.

More complications arise from changing the key or permitting the use of multiple keys.

Protection within the System

The mechanisms just described provide protection of a tape or disk if it is stolen and physically removed to another computer system. Protection can also be provided against unauthorized attempts to read the tape or disk on the same system. The encryption devices can be controlled by software-loadable keys. Each user provides a key to the system that matches his tape or disk.

A more complicated scheme is necessary when files are shared (fig. 2). Data is divided up according to category of information. Each category is assigned to a different encryption key. Each user is provided with a list of keys—the keys corresponding to the data he has permission to access. We call this a need-to-know protection scheme.

Here is an example of how this scheme might be used:

> A bank's data processing system contains records of its savings accounts, checking accounts and loans. Customer names are encrypted using one key, savings account balances using another, and so on. Programs to report to the IRS are given the keys to access name, social security number, and interest amounts. Privacy of account balances and activity records can be assured.

This scheme has several advantages over conventional file access control mechanisms:

- A file can be broken into pieces finer than the normally provided segment.
- There are no large tables to match user names to file names.
- It is not necessary to guarantee that a table access check is performed every time a file is opened.

There are disadvantages to the use of encryption alone to protect files from unauthorized access:

- Encryption does not prevent files from being written over and thus destroyed. Therefore, it would be absolutely necessary to have a good back-up file system.
- In order to protect files from professional code breakers, it is necessary to change all keys periodically. When this is done, all files may be copied and recorded using the new keys.

Protection of Data in Main Storage

This mechanism can be extended to protect data in main storage as in a timesharing system when many users' data are simultaneously present.

BEST COPY AVAILABLE

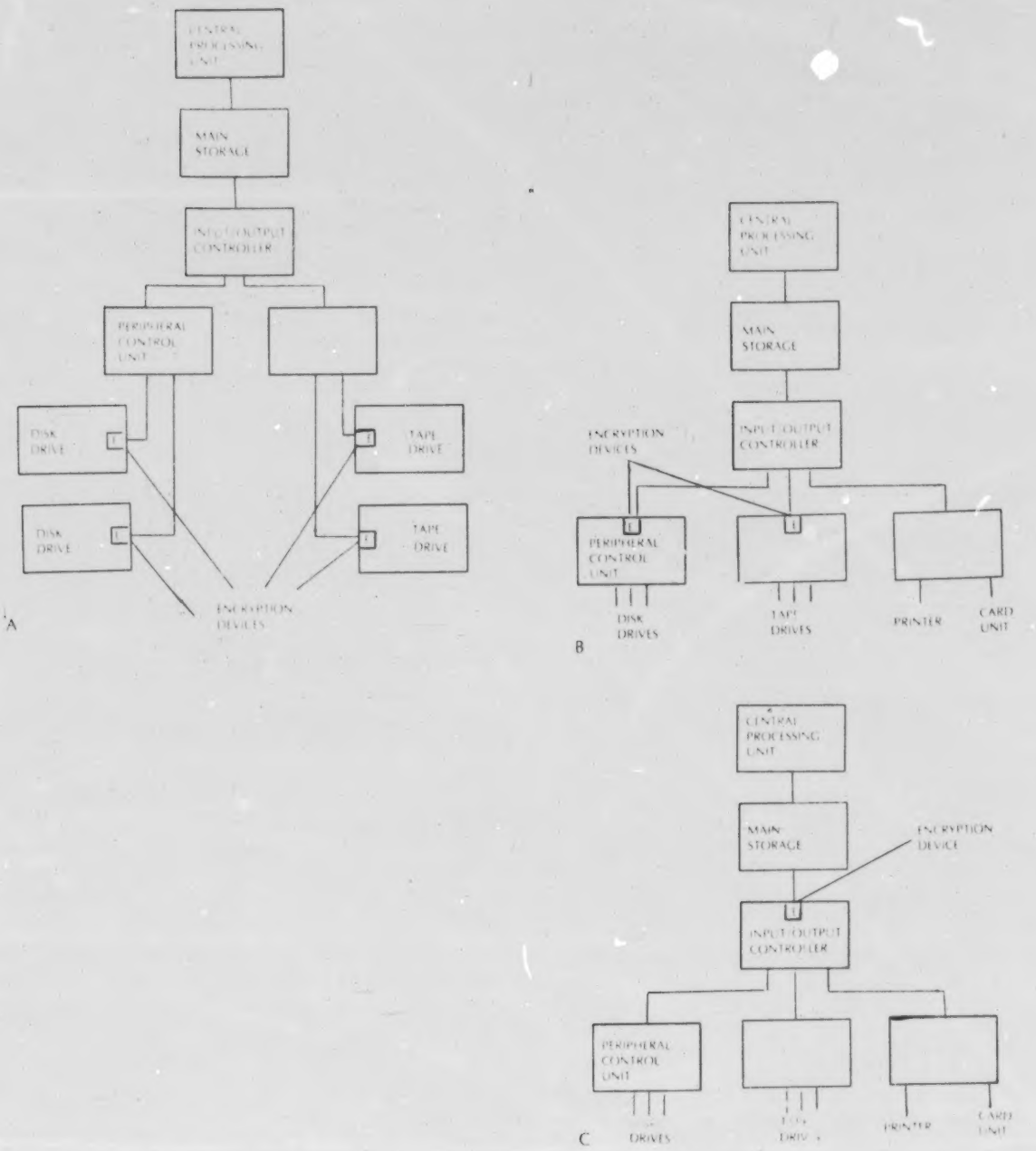


FIGURE 1. *Encryption devices may be placed in the individual disk or tape drives, in the peripheral control units, or in the input/output controller.* More encryption devices are required when they are placed in the disk and tape drives. The encryption device is more difficult to use when placed in the input/output controller.

BEST COPY AVAILABLE

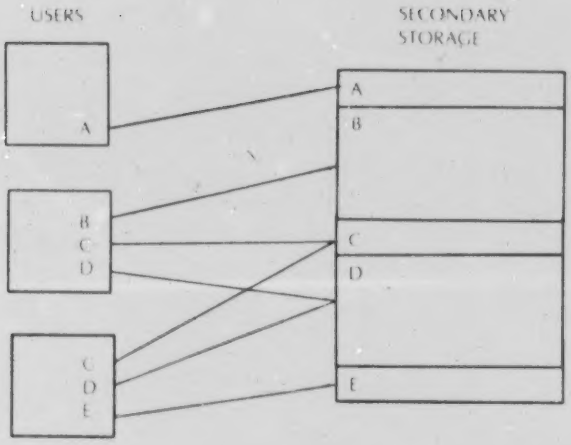


FIGURE 2. *Each user can be given keys to the files he has the right to access.*

First, it will be necessary to put an encryption device between the CPU and main storage (fig. 3A). Second, it will be necessary to find a means of handling control information for I/O devices and data for the printer. This can be done in several ways:

- The channel programs and data for transfer to unit records can be left in decoded form in main storage. This means that the encryption device will have to be turned on and off under program control, adding certain complexities to the CPU program. The CPU, for instance, must know the difference between data destined for the printer and data destined for tape, to be printed later. This distinction may not necessarily be visible to the programmer.
- Encryption devices can be added to the I/O controllers to decode the channel programs and data when necessary (fig. 3B).
- The encryption device can be placed in the main storage unit. Keys and control information would be sent from the CPU and I/O controller at the same times addresses are sent (fig. 3C).

When the encryption device is placed between the CPU and storage it must operate on small fields. This restricts the type of encryption algorithm that can be used. Several keys will have to be kept in CPU registers associated with registers containing addresses such as the instruction counter or base registers. These keys must be loaded and unloaded when the corresponding address registers are changed.

It will be necessary to have tables of keys in main storage, and these tables will have to be protected. We cannot rely on encryption for al of our protection. Even if the tables of keys were encrypted, the key used for that encryption would require protection. So a conventional segment descriptor, base/bounds protection mechanism, or lock and key protection mechanism is still necessary.

What good is it to encrypt data in main storage if we still need the existing protection mechanism? The size and complexity of the existing mechanisms can be reduced. This is an important consideration when it becomes necessary to certify a protection scheme. Present efforts to make a system certifiably secure are directed toward the creation of a security "kernel." The "kernel" is a set of highly privileged programs with the power to impose access restrictions on the rest of the system. The proposed proof of correctness techniques can only be applied to a small amount of code. If a small enough kernel can be isolated then, theoreticaly, it can be proven secure.

Economic Factors

We have encryption devices fast enough and cheap enough for use in communications. These are capable of speeds up to 500,000 bits per second. Software routines that provide encryption secure enough for commercial applications can run at 10,000 bits per second. But tape, disk and main storage have much higher transfer rates. Tapes can transfer data at 2,000,000 bits per second. Disks can transfer at 6,000,000 bits per second and up. Some main storage units can transfer at 200,000,000 bits per second.

Of course, we can improve the performance of most digital devices by increasing parallelism, but size and cost will often rise exponentially. A reasonable upper limit on the size of a commercial encryption device is around 200 TTL packages. This is about four average-sized printed circuit boards as compared to over 100 of these boards for a medium-size central processing unit.

It has been estimated that sequential bit stream encryption devices of this size capable of 10,000,000 bits per second can be built. Such a device would be suitable for tape and disk applications, but for use between a CPU and storage it will be necessary to obtain a device that is both faster and capable of operation in a random access mode.

The Future

Thus we are currently limited by a lack of better, faster encryption techniques and speedier, less costly circuits. Fortunately, we are by no means at the end of our technological capability. Large Scale Integration (LSI) holds a promise that encryption may be feasible in a CPU.

Other problems to be solved are mainly problems of getting more out of encryption schemes and devices:

- Providing master and submaster key capability for distributing need-to-know level information from multiply-encoded files.
- Implementation of the ring properties for multi-privilege access control or the star properties for multilevel government security classifications.

BEST COPY AVAILABLE

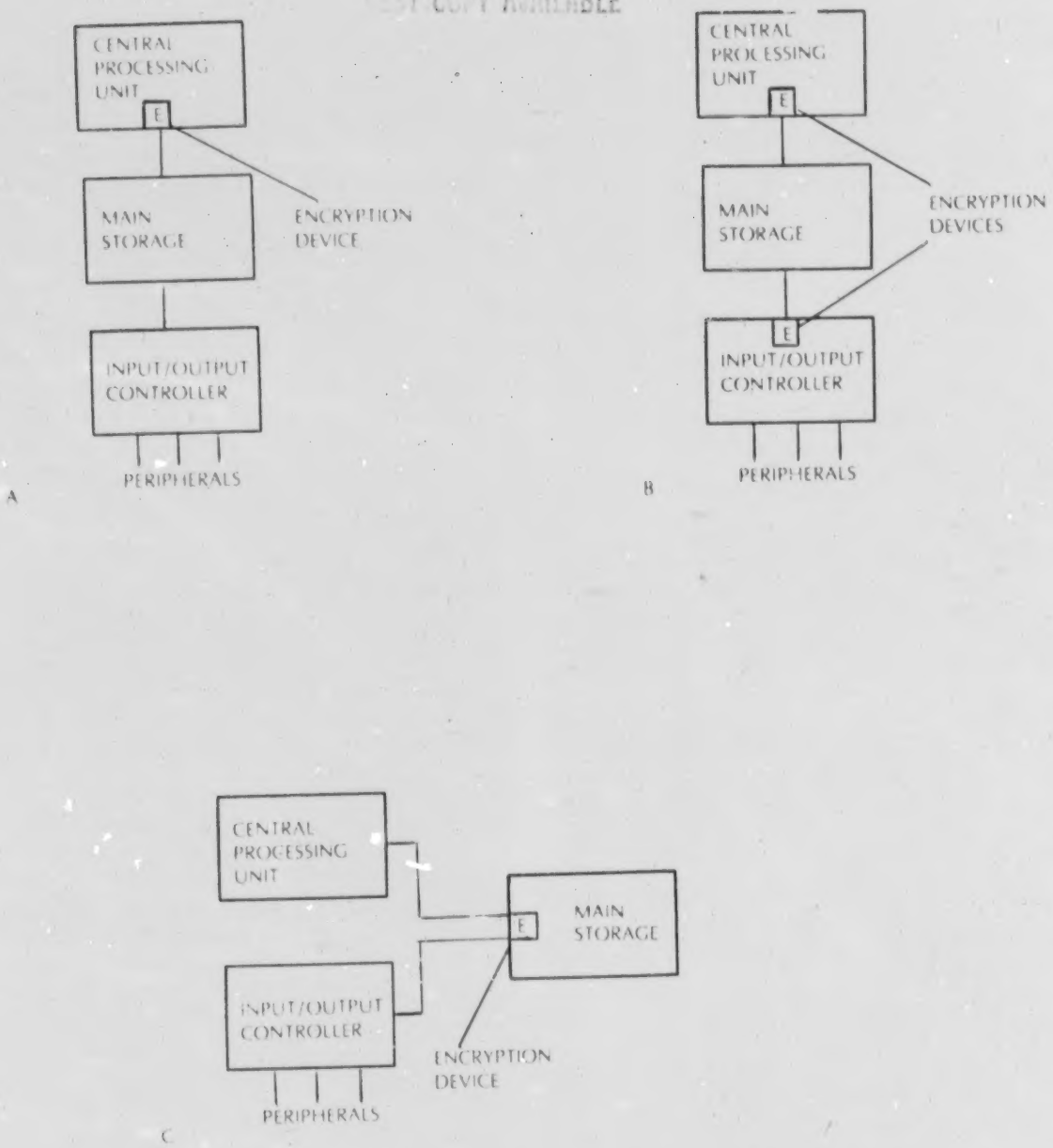


FIGURE 3. *Three configurations for providing encryption in main storage.* Configuration A may not be practical because of complexities in controlling the encryption device The choice between configurations B and C depends upon the design of the main storage/processor interface and the number of main storage modules.

Encryption does help to provide secure systems. However, encryption technology is a specialty of governments. Because commercial demand for secure systems has been low there are too few technicians available to industry. The ultimate success of security architecture using encryption will depend on the willingness of the appropriate government agencies to help develop the algorithms necessary to satisfy the design criteria of data processing machines.

ACCESS CONTROLS IN BURROUGHS LARGE SYSTEMS

Harvey W. Bingham

Burroughs Corporation, Paoli, Pennsylvania 19301

Burroughs Access Control Philosophy

Access control means to authorize access requests for resources or data in a computer system based on an acceptable identification; and to resist unauthorized penetration. Access control should minimally impede authorized use.

We assume adequate physical and administrative security precautions are taken. We also assume the need for sharing the use of the system rather than dedicating its use.

Language barriers are the primary means to realize access controls in the Burroughs large systems, the B6700 and B7700. Language barriers are means to prevent users from being able to directly manipulate nay part of the system. Instead, users only use high level languages, and language processors interpret programs in these languages, and either immediately impose control, or insert control checks for later invocation. The user is unaware of the presence of access controls unless some unauthorized request is made.

Dynamic self-regulation of system resources by the Master Control Program (MCP), or operating system, achieves basic integrity—the system remains in control as work flows through it. Jobs remain separate although resources are shared.

user creates source program file → COMPILER

Any compiler is an object program. It obeys all the rules of object programs, except:

a privileged action is required to make an object program into a compiler.

only a compiler can generate object code.

Access controls are automatically included in all object programs by the compilers.

All object programs are execute-only, they are never data to a user. No ability exists to execute data as if it were object code. Object code never accesses any resource directly. The MCP mediates all resource requests.

The system compilers—DCALGOL and ESPOL, are restricted in use to small parts of the system. Compiler writers do not need these compilers.

The user has a choice of extra levels of controlled sharing if he desires.

Design Objectives

The data processing system should be easy for the user to use. The user needs only a high level language for programming.

Resource sharing should be easy for the user. The MCP should allocate and moderate usage of all physical and logical resources. The owning user specifies privileges to others for his files and/or programs.

Hierarchic structures should provide controlled partitioning internally to keep users separated, except through user-approved interaction points.

Limiting error spreading is essential to real, imperfect systems. Hardware error detection and subsequent isolation should provide control during degradation.

Software Barriers for Access Control

User programming is done in higher level languages only. User programs are referred to as source programs. Every user source program must be compiled into object code before it can be executed.

object program → PROCESSOR
execute-only file

Object programs of other users can only be used if their owner declares them to be public. Like any object program, they are execute-only.

High Level Languages Only

A hierarchy of languages exists to support the users and system. None of them are assembly level languages, nor do any have ways to escape to such a low level language.

Experience with older systems allowing assembly language programming, and execution of data as code leads to the assertion within Burroughs that such systems can never be secured.

Application programmers use the standard languages

COBOL	FORTRAN	EXTENDED ALGOL
PL/1	BASIC	APL

The constraint on these languages is that improper programming can only damage the programmer's own program or files.

All compilers and most MCP and utility routines are written in EXTENDED ALGOL.

Supervisory programmers use a further extension of ALGOL called DECAGOL. This language also includes means to establish controls across users. The constraint is that no error can harm the MCP. Users have included data communications message control systems, workflow management, system operator interface, and rotating memory storage management.

The writers of the MCP kernel use ESPOL, another ALGOL extension. These critical MCP functions include resource managing, input/output handling, and authorization checking. ESPOL permits access to physical hardware and memory addresses, and so is fundamentally dangerous. It is only used where necessary. Links are provided to utilities written in better protected languages.

Master Control Program

The master control program owns and controls all resources. The MCP verifies all user requests for access to any of these resources. The MCP provides resources to each user as needed. When so provided, the user effectively owns them, subject to recall by the MCP. The MCP defines the environment for the user and assures that the environments of the various concurrent users do not conflict. All resource requests are made as a result of compiler-generated descriptors.

A descriptor indicates the kind and extent of the requested resource. The MCP completes a descriptor when a resource is allocated. The descriptor thereafter serves to enforce control. The hardware interprets descriptors automatically.

The hardware access controls apply routinely 100 percent of the time. They provide a secondary level of protection. In normal operation, the software access controls are sufficient.

Memory integrity is basic. Address bounds apply to constrain access to only allocated areas. Tag bits enforce proper use of every memory word: data, program, or control uses are separately indicated. These tag bits cannot be changed by user action.

Error detection and controls sense hardware failure and limit the effects. Both the B6700 and B7700 use parity checks. The B7700 also uses residue, continuity, illegal value or instruction checks.

Interrupts from normal internal or external events and from detected errors return control to the MCP.

Processor state is a further check. Almost all execution is in normal state. Only the MCP can execute in control state the privileged instructions.

System Access and File Access

Access to the system by a potential user is controlled by account identification. The usercode and password are the basic identifiers.

The usercode is a public name; it can be displayed or listed. It is created by the installation and does not change.

The password is a name private to the owner; it can not be displayed or listed. The owner may change it any time. Multiple passwords are permitted to allow multiple users of an account.

Authentication beyond this basic form is the application or installation responsibility. Authentication addresses the questions:

Is the user who he claims to be?
Is the remote terminal or computer who it claims to be?

The process of controlling and protecting account passwords is extremely important. Access, once into the account, is permitted to any files or programs created and thus owned by that account. The account owner determines access privileges for others to any of its files and programs. Thus the account owner controls sharing of his files and programs with other accounts.

Privileged Userdatafile

The system supervisor has a privileged account. That account is responsible for initiating system accounts and assigning them usercodes. The makeuser utility is only usable by that supervisor. It creates the privileged Userdatafile.

Within this file are contained the list of usercodes. For each usercode, the minimum and maximum number of passwords and the transformed values of currently valid ones are included. Password transformations are irreversible, so there is no way to determine actual passwords from this file. The privileged status of each account if any is indicated. The job queues to which the accounts may be attached are listed.

The MCP uses the information in the Userdatafile as one basis for its access control decisions.

Job Queue Classes

An account may be restricted in the subset of system resources available to it. The resources include hardware, software and class of service capabilities.

A set of job queues are provided, each with its own capability list and usercode list.

Any job by a usercode is constrained by the capability list of the job queue to which it can be attached.

File Security

Files are the basic units for an account to retain and share data. The account owns the file and controls accesses to it through specification of file access attributes.

The security type defines the form of access control:

public (class A)
anyone knowing name can access

BEST COPY AVAILABLE

guarded (class B)
owner defines accesses for others

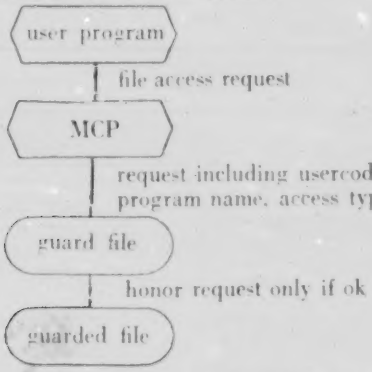
private
only owner can access

The security use defines for public files the allowable use: in, out, both, or secured from use.

The security guard names the private guardfile if the file is guarded.

Guard File

A guard file guards another file. The guard file contains rules for access from other accounts.



During execution of a program under a different account, if an access is requested to the guarded file, the MCP checks the guard file and honors the request only if authorized.

The access alternatives available for granting to programs running under other usercodes include permission to:

only read
only write
read or write
only execute (object code file)

Absence of a usercode in the guard file denies any access to the guarded file—it is secured from that account.

The guard file is private to the user and the privileged MCP. The MCP is its only user.

Limiting Operator Privilege

The supervisory console is a privileged position requiring physical and administrative control. From this position most security checks and access controls are bypassed. This is done so that the operator can participate with the MCP is dynamic self-regulation of the system.

At installation option, the operator can be denied the capability to create usercodes, specify privileged users, or make an object code file into a compiler.

The operator can not determine passwords.

Remote User Security

The central system assumes that physical and communications security for data beyond its immediate environment is provided. A Message Control System (MCS) interfaces and services any remote user. This can be a standard MCS or can be specialized to the application.

The remote user establishes connection and identifies himself with the login function.

For the standard message control systems Remote Job Entry and Command and Edit, a validated usercode and password gives access to that account and all therein as previously described.

For a user-tailored MCS, additional identification and authentication procedures can be developed. These can include terminal self-identification.

The interactive APL language is a good example of a specially tailored MCS that uses its own account name and keyword in place of the usercode and password. The APL user has been provided more selective access protection and control. Different names and keywords apply for account, workspaces and files. Locked functions can hide any knowledge of file names and keywords. An APL application can thus be made secure for others to use it.

The logoff function returns control to a more global process. This process records actions, disconnects, and recovers resources no longer required.

Data Management System

The Burroughs Data Management System maintains and manages a data base in support of multiple user requests for file action.

The standard Data Management System provides management functions including: resource control, security, audit trail, recovery, and contention resolution.

The application designer, building on the Data Management System, can easily specify custom user controls in COBOL. These controls are processes that run before or after file actions for a user. The controls are activated whenever the data base is opened by any user. The controls run as an independent job associated with the data base; not under control of the user program. The application user is unaware of their execution so long as the user requests are proper. The user controls can perform arbitrary functions, including access control and logging.

Obstacles to Penetration

The penetrator must circumvent many access controls.

The primary software controls provide language barriers to misaccess: the MCP, the utilities it provides, the compilers that process source programs, and the controls embedded in the execute-only object code for run-time application.

The secondary hardware controls enforce software controls through memory access checks, and limit effects on error detection.

The owner specified controls are transparent to those users and uses that the owner has specified. The Data Management System conveniently packages many of these optional access controls for easy application.

Summary and Conclusions

The architects of the Burroughs large systems anticipated safe sharing of resources among users. The design is to good commercial practice, but is not claimed to be 100 percent impenetrable. It provides many access controls to resist penetration.

Software language barriers are effective as the first lines of control. Hardware supports these controls by providing a cross-check should error occur.

Any particular application can further specialize the access controls to its needs. Any installation can select those access control extensions it requires and is willing to pay for.

The Burroughs large systems aim has been to provide adequate access controls to resist unauthorized access. Building from this strong base, an ongoing program of product enhancements will support additional access control needs as the market requires.

SYSTEMS ARCHITECTURE FOR SECURITY AND PROTECTION

James P. Anderson

James P. Anderson Company, Ft. Washington, Pennsylvania 19034

Introduction

The purpose of this paper is to outline the role of computer systems architecture in providing computer security and data protection. It will cover the main trends in computer architecture as these impact the security problem.

The primary impetus to modifications in computer architecture in the past has come from considerations of efficiency. From the first introduction of "B"-boxes to provide efficient address modification for calculation loops to modern computers with multi-state operation modes and instruction (sub) sets specialized for computation or data handling the emphasis on systems architecture has been efficiency. The past decade has seen the rise of systems architectural features aimed at improving the efficiency with which a computer system can be used in production environments. Thus, we have today computer systems designed to handle multiprogramming, multiple job streams, on-line operations, interactive programming and the like. The main thrust of these developments has been motivated by a desire to get the most use out of what has been an expensive resource.

These operational capabilities also made it possible to efficiently share information and program resources among a variety of users of a system. However, in order to share these resources efficiently, it became necessary to make them available on demand. Further, the requirement for sharing placed a burden on the computer system of having to control who would share what, and how the sharing is to take place.

Until there were computer systems with the functional capabilities associated with resource sharing, the primary security mechanism that existed was isolation. The isolation approach physically separated sensitive data from all others, and guaranteed the integrity of that data by running programs that referred to it in isolation. When the processing of the sensitive data was complete, the file media were removed from the system, and the machine cleared of any residue in memory to preserve the isolation. As will be discussed, isolation as a security technique is being rediscovered.

The designers of early third generation computers of a decade ago focused on the potential for chaos that could exist in multi-programmed systems if there were not some means available to prevent user programs from interfering with each other and with the operating system. As a result of this (and other considerations), these systems had base and bound (sometimes base registers and storage locks) registers to establish the beginning and extent of a user program. Attempts to reference outside of these limits by a user program would trap to the supervisor for disposition. For some time this was thought to provide adequate security for a system. However, it is interesting to note that none of many penetration exercises have attempted to bypass the base-bounds registers directly; they have instead exploited the fact that the supervisory program requires full memory addressing capability, and that such addressing is granted to

(a) access parameters in user space
(b) return results to user programs

even though the functions being called are common service functions rather than resource allocation and management functions.

Isolation as a Fundamental Security Principle

Just as the major impetus for architectural innovations in the past was efficiency of operations, the impetus of architectural innovations for security and protection is to provide isolation mechanisms that cannot be bypassed by users exercising normal (user) programming control of a system. Further, in examining the problem, it becomes clear that the "users program" is not just the code he has written, but includes all of the supervisory, monitor or operating system programs executed on his behalf.

If the isolation principle is not extended to the supervisory programs that provide the "environment" for a program, it is then necessary to be able to prove that these (considerable) programs are secure and implemented correctly. This is a task most people will accept as impossible with today's state-of-the-art.

However, there are means of avoiding the problem by including the bulk of the operating system and its

BEST COPY AVAILABLE

supervisory or monitor programs within the isolation envelope surrounding the execution of programs for a given user. Once the idea is conceived, the problem becomes one of finding efficient mechanisms to accomplish the desired result.

While there are numerous reasons other than security or protection for adopting certain architectural approaches for systems designs, the balance of this paper will be concerned with those derived from consideration of security and protection.

Security Versus System Functionality

It is well recognized that the degree of security threat a user of a computer system poses is a function of how that user is able to make use of the system. This is often couched in terms of whether the user can program the system, usually in machine language. The concern with the functionality provided to a user is focused on the fact that with a programming capability, a user may be able to exploit any errors in design or implementation of the operating system, and escape from the isolation envelope surrounding his program. Alternatively, even if he is effectively contained in his envelope it may be possible for the malicious user to cause the operating system to supply data about itself or others users on the system by supplying unexpected parameters in system calls, or executing system functions out of an expected sequence. Rather than speculate on the methods that might be available to a malicious programmer, it is sufficient to note that with an increase in functionality provided to a user there is need to include the operating system itself in the isolation envelope or to assure completely the correctness of its design and implementation.

Where the user of the system does not have the capability to execute arbitrary program sequences, as in a system that interprets transaction parameters, the user is in effect isolated by the application itself.

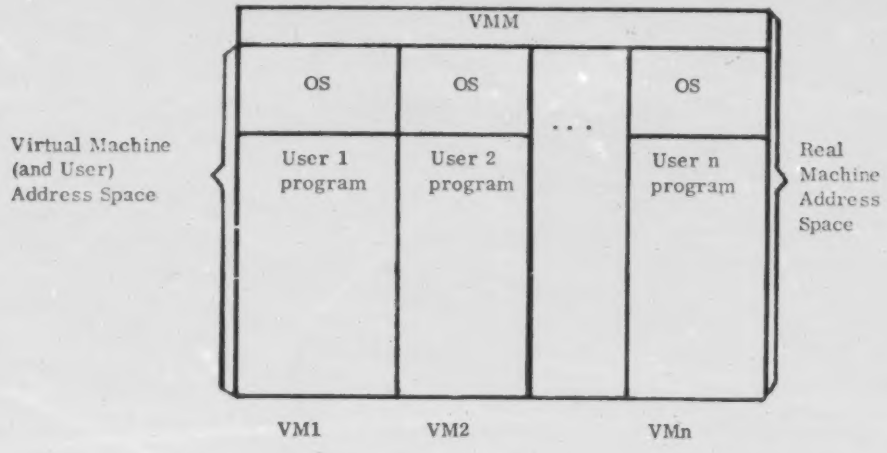
Architectural Approaches for Security

There have been basically two architectural approaches to provide the type of isolation discussed above; virtual machine systems and virtual memory systems. The latter, not to be confused with the marketing terminology of some manufacturers, are frequently referred to as descriptor-based systems.

Virtual Machine Systems

The virtual machine system approach to creating an isolated environment is characterized by designing a small operating system and using the technique of multi-programming to make available to each user an interface to the computer that is functionally equivalent to a complete "raw" or "bare" machine and in which there are no restrictions on the type or category of instructions that can be executed. This is contrasted with the conventional two state operating system approach which, in order to protect itself restricts the user from executing certain instructions; notably I/O, and those others that are specified as "privileged" (to the supervisory state of the system).

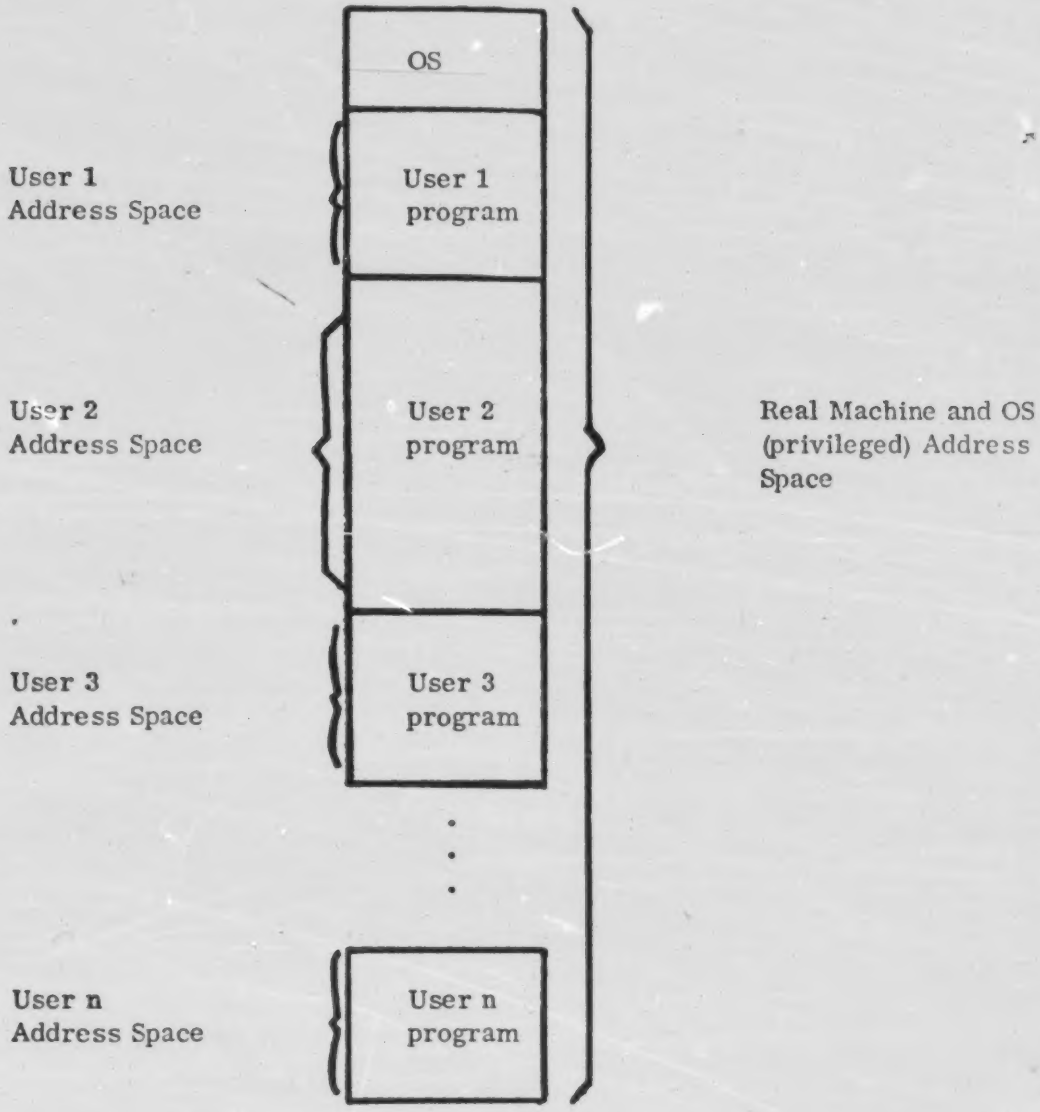
The operating system that creates this environment is known as a virtual machine monitor (VMM), and consists primarily of programs that provided interpretive execution for privileged instructions that are trapped to it, as well as the minimal controls to initiate and discontinue virtual machines and the controls to effect time-multiplexing of virtual machines on a single set of hardware. A major portion of VMM's is devoted to interpreting I/O (for integrity and correct operation on a VM) and simulating to the VM such controls as interrupts, error indications and the like. With each user having functionally a complete "raw" machine of his own, in which it doesn't matter whether the instructions being executed are privileged or not, it is of significantly less security importance whether the operating system running in a virtual machine is correctly designed and implemented, since in the extreme, each user can be provided with his own copy of the operating system, thus, completely closing off any possibility of interaction between two virtual machines. The form of a VM operation is illustrated below:



This is contrasted with ordinary multiprogramming use which can be represented as:

grammer by isolating him in a single (virtual) machine. It also eliminates the need to be concerned with

BEST COPY AVAILABLE



The virtual machine approach described here is one that shares only hardware resources, in a way that makes a modern version of the isolation technique feasible.

From a security viewpoint, the VM approach provides the necessary protection from a malicious pro-

the security worthiness of an existing operating system, since in the VM, the operating system can be thought of (and implemented) as belonging to a single user.

Because the VMM need be concerned only with the functions of simulating privileged instructions and the

controls needed to effect initiation, multiprogramming, and termination of VM's, it can be quite small compared to typical operating systems, and relatively simple. These factors are important, since they make it possible to subject the VMM to thorough debugging and validation of the design.

Perhaps the most important aspect of the VM approach is that it is one that can be applied to existing two-state systems with the (relatively) minor hardware modifications necessary to trap all instructions that refer to or rely on the state of the system or initiate I/O operations.

It is not expected that the VM architecture described above provides quite enough capability for most users. In particular, it is necessary to provide secure (protected) communications between VM's in order to permit data or program sharing. This could take the form of a virtual inter-computer channel and/or a shared virtual file media. Such a capability could be used to implement controlled sharing of data bases (in addition to the unique data bases included in the basic concept) in a separate virtual machine.

Finally, the question of the most efficient method of mutiplexing VM's on a set of hardware depends to some extent on whether it is possible to designate some part(s) of the VM's memory as execute only (i.e., read only as instructions; no write); in which case separate copies of a standard operating system might not have to be provided to each user.

The virtual machine system architectural approach is perhaps most applicable in service center applications where hardware resources are shared among different organizations; each with a need to protect their information and program resources from people outside of their organization. Each organization could be assigned a separate virtual machine. The functional needs of the organization for time-sharing, remote batch, teleprocessing and the like can be met by the capabilities of the standard operating system for the base machine run in a virtual machine. Optimization of an operating system to meet specific functional needs of an organization is easily accommodated without penalty to other using organizations.

The virtual machine approach provides a method of sharing hardware securely; it provides no mechanisms for sharing other (data or program) resources. These have to be developed within the VM framework. Where the sharing of data and program resources is minimal, the use of pseudo inter machine channels to effect access between consenting systems is adequate. Where more comprehensive sharing of program or data resources is required, as in general utility systems, other approaches appear to provide greater efficiency.

Descriptor Based Systems

In the preceding section, it was stated that VM systems provide isolation by simulating to each user a programming environment that is essentially a complete raw or bare machine. Another approach to isolating users is to use a descriptor architecture to provide each user with a totally independent address space, in the familiar context of an operating system environment.

The original motivation for descriptor-based systems was limitations of real memory on early computer systems. This had been a problem ever since computers were first introduced. Ingenious variations on overlays were employed to overcome this limitation and reached a high state of development through the language formalisms describing the boundaries for overlays (COBOL sections and ALGOL blocks). Descriptors were important to these developments by providing an extended form of indirect addressing that made it possible to compile each portion of a program independently of the others in a single pass over the program text. References to other program parts were directed to descriptors which contained pointers to the location of the required part and ancilary information about the part. All of this activity was going on in the ferment of the early developments in multiprogramming. The developments reached a culmination in the development of the Burroughs B5000 in 1961. Subsequent to this development, the GE 645 was developed in the multics project at MIT. Descriptors play an important role in this machine as well as in the Honeywell 6180 and other systems under development at the end of the decade.

A descriptor is a computer word that acts as a form of extended indirect address. When a descriptor is referenced, control bits contained in the descriptor are interpreted in hardware to mediate the completion of the reference. The mediation that can be accomplished includes automatic fetching from secondary storage data and/or program parts recognized not to be in main storage, automatic type conversion and the like. Because the descriptor is an economical way of preserving the attributes of the object being represented, the reference limitation requirements for the object (read only for execution, read-only, write, append, etc.) are included as part of the control. This is an important design point because it makes it possible to represent the protection requirements of an object in its descriptor and be assured that there will be automatic hardware controlled validation of all reference to all objects of a program represented by a descriptor. This property makes it possible to use descriptors to implement self-protecting systems.

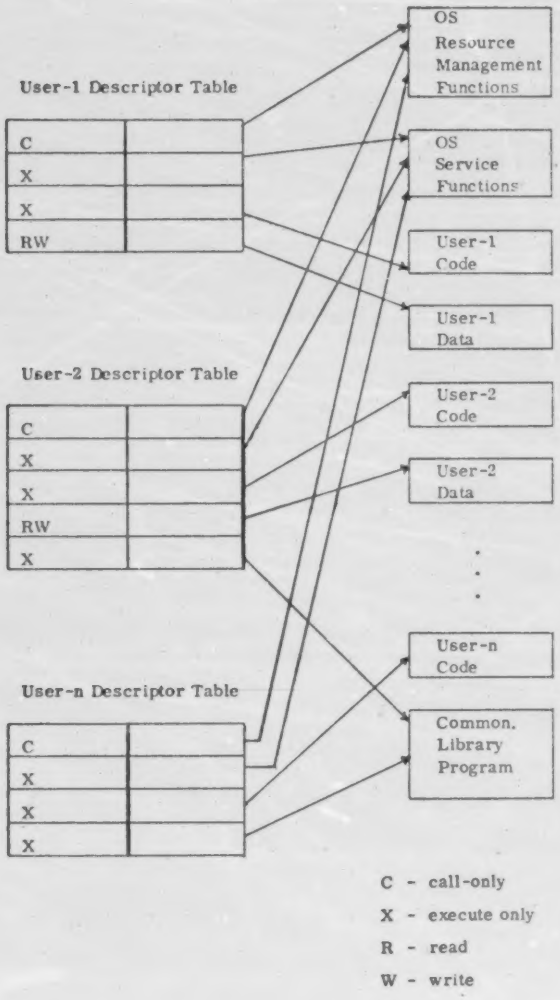
If all of the objects of a program execution are represented by descriptors (including the implied parts of the operating system) and the descriptors are protected from alteration by a user program, the user is isolated to a virtual address space (memory) defined by the set of descriptors used to represent his program.

Descriptor protection can be accomplished by providing extra (non computational) bits per word to distinguish descriptor words from data words (as in the B5000 et. seq.), or by collecting descriptors in a table based by a register that is implicitly involved in memory references, yet which can be set only in a privileged state. In either case, the descriptors cannot be manipulated by a user programmer, thus, providing the necessary mechanism to protect the integrity of the isolation envelope.

BEST COPY AVAILABLE

With a descriptor capability, a variety of interesting systems can be built. However, the major benefit available from use of a descriptor controlled virtual addressing approach is the ability to provide precise control over sharing of programs or data by including the object to be shared as a descriptor in the sharing program with the protection control bits set to control how the object may be referenced.

A highly simplified representation of how sharing and isolation can be accomplished in descriptor-based systems is shown in the figure below. The diagram indicates that each user program can execute the operating system service functions and its own code within the addressing context established by the descriptor table, can cal on the operating system resource management functions (e.g., to obtain additional storage, or perhaps another program dynamically), and read and write its own data. Common library programs can also be shared among different program as can data.



What Else is Needed?

Both the VM and descriptor-based systems provide the basic ingredient of security and protection in resource-shared systems; isolation. For this reason, both 'schools' of architecture are being pursued in connection with secure computer systems. Beyond the basic mechanism for isolation, both approaches need additional security components to control initial access to the respective systems.

Additional Security Components for VM's

The primary security control needed in the virtual machine approach is an authorization mechanism that validates a user's authority to initiate (create) a virtual machine. The mechanism must be based on some form of authenticated unique identification. Because it controls initial access to the virtual systems the authorization mechanism must be an integral part of the VMM, and protected from alteration by VM's running under it. If virtual machines are allocated on a per-user basis, the authorization mechanism will also have to maintain a list of all possible users and the program and data resources belonging to each, in order to establish the correct configuration of virtual machine.

If virtual machines are shared, as in a service center for example, the VMM would only have to maintain an authority to initiate a VM (if it is not delegated to the center operators). Authorization to use a VM or its program and data resources can be handled by the authorization mechanisms available in the operating system for each VM.

Additional Security Components for Descriptor-Based Systems

The descriptor-based systems also need authorization mechanisms to control use of the system. However, because they present an operating system environment to user programmers (as opposed to a bare or raw machine environment provided by the VM approach) they must also include authorization mechanisms to control sharing of program and data objects contained in the system. Both of these mechanisms, the additional mechanism that establishes and maintains the users 'context' (i.e. descriptor table), and the descriptor tables must be protected from alteration by user programs.

Summary

The major systems architectural approaches to security and protection implement the isolation principle. In the virtual machine approach, users are provided isolated virtual machines. In the descriptor-based virtual memory approach, users are provided isolated independent virtual address spaces. Both approaches must be augmented with used identification and authorization mechanisms to provide a complete secure environment. The VM approach appears especially attractive for providing the basic system self-protection needed for environments such as service centers primarily concerned with sharing hardware resources. The descriptor based virtual memory approach has greater applicability where on-line time-sharing or utility-like systems are needed and where there is a major requirement to share programs and/or data.

References

1. Buzen, J. P. Gagliardi, U. O., Introduction to Virtual Machines, Honeywell Computer Journal, Vol. 7, No. 4, 1973.
2. Organick, E. I., The Multics System (The MIT Press, Cambridge, Massachusetts and London, England, 1972).
3. System/3000 External Reference Specifications (Hewitt Packard Co., December 1971).
4. Burroughs B6700 Information Processing Systems Reference Manual, Burroughs Corp., Detroit, Michigan (1969).

PRAGMATIC APPROACHES TO SOFTWARE SECURITY

Richard L. Caplan

Advanced Computer Techniques Corporation, New York, N.Y. 10022

I work for a consulting firm. Consultants are forced to deal with the world as it really exists and it rarely conforms to theoretical models. I would imagine most of you are similarly involved in one way or another with existing installations that have multi-million dollar commitments in hardware and user programs. I am going to describe three case studies that demonstrate my company's activities in a security context involving actual users like yourselves. I am going to talk about strategies and products that we have had to develop in order to solve existing problems, and I will attempt in turn to draw conclusions about the nature of software security in general.

At best, computer security must be viewed as a five-dimensional problem. The first and most obvious dimension is physical security which I have euphemistically labeled "the fox in the chicken coup" problem to suggest the fact that when we lock our machine room doors we are essentially locking our insecurities in since the people that we may have the most reason to fear are our own technical and operational personnel.

This intentionally provocative comment should immediately suggest the second security exposure and that is a "motivational" one. It is reflected by a need for evaluation and monitoring of the emotional stability of technical personnel on an on-going basis. I find

myself particularly well-suited to comment on this point since I have had relatively long hair and somewhat unorthodox political views for years, and I therefore have personal knowledge of the tendency of EDP management to consider programmers and analysts as basically a weird lot. And yet there is, surprisingly, a lack of concern manifested by these same managers for the reliability of subordinate technicians in terms of their handling of sensitive data files and computer programs.

The third security exposure I have labeled "communicative." It involves the propagation of cross-talk or "noise" within existing official communication channels (or subrosa unofficial paths) among DP professionals. This threat to computer security consists of the uncontrolled availability of vital information and its dissemination by mouth or written word between the technical and user communities.

The fourth security exposure has been labeled, for want of a better word, "systematic" and applies to the faults that may be found in what we buy or rent from the computer manufacturers. While we all hope, no doubt, that the understanding and heightened technical awareness of the manufacturers will tend to minimize the faults in computer products, both hardware and software. We must be cognizant of the fact that the development of these products is often predicated on the performance of delicate balancing tests or tradeoffs of cost effectiveness, which are conditioned both by state of the art technology and the vicissitudes of the marketplace. We know both as users and consultants that we are often the ultimate discoverors of such faults within computer products, and our efforts to communicate them precisely to the manufacturers represent a substantial service to the industry as a whole.

The fifth and last major computer security exposure I have designated as "constructive." It arises through the propagation of security gaps within applications programs and user software which we create ourselves within the total environment supplied by the computer manufacturer. It is to this area of user program security that the balance of this address will be dedicated.

Let us now turn to consider the three practical case studies. The first of these involves interface management. In the computer world "the manual is the message" to coin a phrase. The complexities of an operational computer system, with its nested layers of procedure, software, and hardware, are generally reflected within written descriptions of capabilities so that to the user the system appears to be a collection of manuals. In this sense, every real system defined by a set of manuals is truly a virtual system, the details of which can be functionally manipulated by changing the written description within limits loosely established by the actual implementations of the hardware/software environment. By controlling the image of the machinery as it appears to different users through documentation, one could go a long way toward reducing the security exposure incident to uncontrolled technical cross-talk. One might in effect manipulate ambiguity in the service of security within the contents of manuals so that specific sub-sets of sensitive information would be presented to a particular audience only on a "need to know" basis as determined by job function requirements within the DP context.

In summary, my company tends to view a significant component of the total software security problem as the adequate definition and control of system documentation. In this regard we approached the creation of integrated documentation system for a computer manufacturer by first undertaking a need-to-know analysis geared to the various classes of potential users of the documentation. Each user's informational requirements as well as existing paths of flow of technical data within the on-going operation were analyzed. We were able to process the results statistically and to determine with relative accuracy the classes of data which could be profitable excluded from various manuals to improve both readability and usefulness, and at the same time increase total security by denying to any individual more information than was explicitly necessary for the performance of his role. To do this we created the concept of a documentation "template." This is in essence an outline of a document format designed to fit the needs of a particular audience. Thus, there may be more than one kind of manual describing the same subject if audience requirements are variable. Each template initially took the form of a gross table of contents for a single document aimed at a single audience. Of course, the price paid for increased security was some degree of redundancy between manuals describing the same system as seen by different audiences. Over the years a master file of these templates has been created and detailed instructions have been developed for driving the technical "flesh" needed to fill out each skeletal structure. We have refined this approach to the point where it can be meaningfuly automated so that relevant system documentation is stored and maintained as an adjunct to actual program libraries on mass storage devices. This approach insures that modifications of the program cannot be completed without corresponding modifications to the descriptive documents. It also allows user access control, presently restricted to the programs themselves, to be applied to their documentation as well. Availability of audit trails and access lists to documentation may be extremely valuable in determining those individuals who have sufficient access to technical information to represent potential threats from a security viewpoint.

These techniques for the control of technical documentation are fully justified by the fact that technical personnel are in no position to outwit a complex software system unless and until they have detailed knowledge of how the existing system operates. This is only available through manuals or inputs from other technicians who have access to manuals. Therefore, by controlling this information, we minimize if not totally eliminate the temptation to manipulate the DP environment for personal gain.

The second case study involves the development of a sophisticated, real-time environment simulator for use in testing an on-line reservations system. While systems testing per se may not, on the surface, appear to be closely related to security, it is my judgment that

software insecurity is directly traceable to inadequate program testing. In particular, if we have no viable techniques for accurately determining what a program does, it may be virtually impossible to determine if and when the program is doing something extraordinary which represents a breach of security. In this regard, complex real-time systems present what initially appear to be insurmountable system test problems. While initial algorithms may be reasonably tested within a laboratory context, final testing must involve manipulation of both the temporal and data content dimensions if all processing paths are to be validated. This requires the production of statistically representative transaction samples which fully exercise all of the features of the system under test. To accomplish this on a manual basis is virtually impossible, particularly when the number of remote terminals is in the hundreds and the number of valid transaction types could and did fill a book.

While we had done a substantial amount of theoretical toying with a real-time environment simulation concept, we received our initial impetus to develop such a tool when a major company with a reservation system asked us to come in and help them check it out in an economically and technologically reasonable way. We propose the direct coupling of two processors, one of which would house the user's application program and TP monitor and the other the environment simulator written by us. They would be connected by a patch panel capable of creating the impact of variable sets of remotely terminated communications lines of representative band widths. This would allow dynamic modification of the on-line remote hardware environment from test to test. The environment simulator treated each transaction as a linguistic sentence with each message and response a grammatical element in the total sentence structure. Using this processing technique and a nodal, tree structure tracing algorithm, each transaction was reduced to a transition diagram. Each of the diagrams was in turn related to actual message syntax structure which, in turn, contined variable data elements which could be drawn from a dictionary. The simulator was capable of generating transactions for submission across lines in real time and dispatching them in a manner which reflected realistic expectations of final operating line loads and initiation patterns.

Responses generated by the user's system under test could be checked and deviations recorded along with message receipt times and hardware error statistics. The resulting log was interpreted off-line to determine system performance, both in terms of validly processed transactions and decay in response time due to increased line loads. The environment simulator did not only generate valid message sequences, but allowed intentional statistical manipulation of transaction components into unacceptable transactions in order to determine whether the target system was capable of disinguishing improper conduct on the part of terminal operators. In this way a host of unforeseen bugs was uncovered and major security flaws were eliminated by providing an exhaustive, statistically based testing mechanism. In this manner a higher level of user created software security was assured.

Turning now to the last and most sophisticated of the three case studies, let us consider the problem of measuring the conformance of user created application programs to their functional specifications. The traditional approach to testing of an application's program must be viewed as a self-confirming prophecy. When you send a programmer out to develop a system whose functional specifications you have supplied, he certainly will not come back to you and tell you that the system works unless it does at least what you have told him it is supposed to do. Unfortunately, the vital security question is not whether it does this much, but rather, does it do more than you told the programmer it was supposed to do. In other words, has the developer of the program, either inadvertently or by design, added to the functional capabilities of the final product features which represent a threat to the integrity of your installation or your data files. Placing the program into the job stream on a production basis clearly is not an efficient way of determining if such hidden capabilities exist. Unfortunately, however, the manager often has no recourse but to place the program in service and hope that six months or a year later he does not discover, at great expense to his company, that the program has all the while been creating a financial nest egg for the programmer or accumulating proprietary data for sale to competitors using the distribution facilities available in the company mail room. Faced with this vexing problem, which is characteristic of virtually all applications development environments, my company has set about to define an algorithm capable of interrogating an object code program to determine whether functional specifications traditionally supplied by the programmer (system specs, flow charts, etc.) are in fact telling the truth about what the program does. We have in effect come up with a design for a program "lie-detector" designed to assure management that specifications are an accurate reflection of program algorithms. Of course, such a system cannot be developed with a hundred percent accuracy. If this were logically possible, such a system would be capable of writing the programs in question without programmer intervention based entirely on functional specifications provided in the English language.

What we have developed, however, is a system capable of providing meaningful statistical clues as to the validity of the routines of a program in terms of access to data fields within records and the manipulation of the data items in the service of goals defined by the program developer. Using our approach it becomes possible to determine whether a program accesses data fields which it was not required to address, whether it performs arithmetic operations upon data items which were not defined within the intended algorithm, whether it causes the permutation of record formats or attempts to access files which are theoretically unavailable, and finally, whether it includes routines whose functions appear ambiguous enough to require explanation by the programmer who performed the coding. The nucleus of our algorithm is a sophisticated flow-

charting system capable of establishing all of the paths through an assembly language program based on the extrapolated contents of index registers and the potential value of address contents utilized by the code. Using this algorithm, which has already been developed, we are on the verge of providing a most powerful tool which can provide DP managers with an accurate, periodic audit of the functional status of their applications and software. The mere availability of such a powerful tool will serve to disuade the dishonest or adventurous programmer from attempting to imbed within a legitimate application a self-serving subroutine or to plant disruptive faults which may be triggered by chance events cognizable by the program, occurring months after he has left the installation or quit the company. We hope that this type of system will find significant use as an adjunct to the classical audit function performed by certified public accountants of the economic integrity of commercial companies. By being able to get an accurate view of the status of applications programming, these auditors will be in a better position to measure the validity of figures which the company's computers provide.

In the limited amount of time made available to me, I have tried to show how the consultant approaches complexities of computer software security on a pragmatic basis in response to pressing user requirements. By concentrating our attention on improvements in the testing of user created programs as well as the structuring and control of user technical documentation, we feel that we are taking a significant step toward achieving an across-the-board improvement in existing computer system security.

INFORMATION AND SECURITY MANAGEMENT

Joseph F. Cunningham
Executive Director, Association for Computing Machinery
1133 Avenue of the Americas, New York, N.Y. 10036

Good afternoon Ladies and Gentlemen. For many years, it was popular to say that "everyone talks about the weather but nobody does anything about it," a saying with may no longer have the same significance since the advent of the computer has permitted a better job of forecasting the weather so that we really know what is coming. To bring this analogy into the current arena, one might replace weather with privacy and security and indeed it seems there has been a lot of conversation about it until finally the National Bureau of Standards has attempted to synthesize what has been going on.

As you well know, the subject starts with attempting to identify and define the term "privacy" and then the rights associated with it. It passes on then to the discussion of means for preserving these rights including some rather exotic legal notions. If the legal actions proposed so far have been exotic so too have many of the safeguards designed to assure the safety of computer based systems. One notices with amusement that there does not seem to be an equal amount of effort directed towards protection of those systems which are not computer based.

Yesterday, Bob Rector outlined the broad dimensions of professional responsibility for reacting to the national issues of privacy and of computer security. Today, I would like to assure you that ACM has been reacting and acting.

In cooperation with the National Bureau of Standards and with financial assistance from the National Science Foundation, ACM has been assessing the technical fundamentals which support action programs in several areas of national importance. It should be of interest that these efforts have been underway since late 1970. It should be of no surprise to this audience that highest priority was given to Privacy and that second priority went to Controlled Accessibility. These areas have no instant answers, only instant "experts." We are working hard on getting the answers and will be working on them for a long time.

Let me give you a progress report as of March 1974.

In the Privacy area, the technologies are legal, social and political sciences. The issues are public policy. As many people, including the President, are saying, the time has come for action rather than for more studies. More than a year ago, NBS and ACM assembled a planning group here in this building to explore the alternatives for action. The group was drawn from an exceptionally wide range of interests, and it rather quickly agreed upon a structure for providing sound, fundamentally accurate information to governmental, private sector, and public interest agencies working on policies with respect to Privacy.

This structure has been evolving into finished form through the efforts of a sub-group composed of Alan Westin, David Martin of HEW, Walter Carlson representing ACM and NBS.

In the area of Controlled Accessibility, the progress has been more rapid. A planning group convened early in 1972 by NBS and ACM defined five segments of technology of importance to data confidentiality and data security. In December 1972, about 70 of the country's knowledgeable persons—including some in this room—were brought together to state what they could agree upon in each of the five segments as being sound, fundamentally accurate information. As the people attending the November conference and this one would know, the field is far easier to describe in terms of unknowns and uncertainties than it is in terms of fundamental precents. The NBS staff has been sifting the kernels of lasting wisdom from the positions adopted by the December 1972 attendees, and one of the

products of this effort will be in the form of an Executive Guide to Computer Security that will contain information with respect to questions that top management wants answered in organizations using computers.

But I submit that much of the work accomplished to date, and more yet to be defined, can possibly all be for naught if we do not learn the significance, terms and implications of proposed or actual legal remedies and resolve how the technology can and must be applied from the systems point of view so that we may manage alertly.

And now let's go to the speakers who make up this panel.

RISK ANALYSIS IN PLANNING FOR PHYSICAL SECURITY

Robert V. Jacobson

Sentor Security Group, Inc., 17 Battery Place, New York, N.Y. 10004

Too often reliance on rituals and amulets is substituted for rational thought in developing security programs. This is particularly risky when dealing with computer systems since potential losses may not always be obvious. For example, if we keep $1 million dollars in our money vault, it is clear that the limit on our potential loss is $1 million dollars. But what about a stolen reel of computer tape? The replacement cost wil be about $15. It may have cost $50 in computer time to compile an engineering analysis program and record it on the tape. The cost to write the program might exceed $50 thousand and the potential impact on profits might exceed $5 million if the program fell into the hands of a competitor. In short while the cost of the stolen item might be only a few dollars, the impact on the organization might be measured in millions of dollars. And there is no way to tell the value of a computer system asset by direct inspection.

The first step in the rational approach to security planning is to define computer system security as two specific performance parameters:

- protection against losses caused by delays in completing assigned data processing tasks, and
- protection of assets against loss, theft or misuse.

Every data processing task has some time constraint on its completion. If an accident, sabotage, power failure or other mishap delays processing, the organization suffers a loss. Generally speaking, the longer the delay the greater will be the loss. Of course, some data processing tasks are much more time urgent than others. But if no loss results from a delay, then the task need never be done. The sum of the losses estimated for all the tasks assigned to a computer system provides a means for gauging quantitatively the losses which result from delays.

To complete the picture, we must determine what events could cause delays and for each such event type we must estimate the probability of its occurrence, perhaps on an annual basis, and the mean duration of the resulting delay. Using these two estimates and our estimates of potential losses, we can estimate the expected losses from delays on an annual basis for each type of damaging event.

Loss, theft or misuse of assets controlled directly or indirectly by the computer system can be costly to the organization. It is helpful to think of three classes of assets:

- Physical assets of the computer system; computer hardware, air conditioning and electric power equipment and other required units. Note that while the value of the contents of the typical office will be in the range of $10 per square foot, the same value for a computer room might be as high as $2000.
- The system "software": programs, data files, documentation and other simiar items particular to the computer system. These assets can be costly to reconstruct if lost, may be attractive targets for theft or may have special privacy considerations.
- Money, negotiable instruments, goods and services may all be controlled by a computer system with the result that it offers a potential route for fraud or theft.

It is important to review the computer system as a whole to assess properly the value of the physical assets and then to review each of the assigned tasks to establish the value of each of the associated programs and data files and to evaluate the potential for fraud or theft of other assets via the computer system. Then just as was the case with delay losses, we must determine what events might lead to losses, the amount of the loss and the probability of occurrence for each such event. These estimates will lead, finally, to an annualized loss expectancy estimate for each of the three classes of assets.

When we have completed these two estimates . . . . the expected losses from delayed processing and the expected asset losses . . . . we can see clearly which are the significant threats and which parts of our computer system have the greatest potential for loss. This yields several powerful advantages in developing the physical security program:

- Security measures can be focused on the areas of greatest need.

- The estimated loss expectancy provides a gauge for determining a reasonable level of expenditure for protective measures.
- The relationship between physical security measures and other aspects of the security program is clearer and fund allocation can be made more effectively.
- A policy statement for the computer security program can be constructed with some precision to address the true security needs of the organization.
- Finally, the security audit program will have greater value since it can draw on the risk analysis to identify the areas which require the most attention.

In summary, the key point is this: Unlike the typical risk situation where the value of the potential loss is usually selfevident, the loss potential associated with a computer system can only be determined through a systematic and comprehensive quantitative assessment of the risk. Guesswork at the very least will lead to misuse of available security funding and in the worst case might expose the organization to disaster.

SECURITY CONSIDERATIONS IN INFORMATION SYSTEM DESIGN*

Steven B. Lipner
MITRE Corporation, Bedford, Massachusetts 01730

Introduction

This paper presents a brief discussion of security considerations in the design of computer-based information systems. The objective of the paper is not to provide a complete technical discussion of each issue raised, but rather to present the reader with an overview of such issues and to motivate the consideration of these issues in the design of information systems that must handle sensitive information.

One major point that wil be made by this paper is that the handling of security in a computer-based information system is at best a difficult problem. However, deferring consideration of security issues has never been shown to be a viable way of handling the problem. Security problems that could have been resolved by an early design decision have a way of returning to haunt the designer who ignores them. The designer is best served by addressing security as he designs the system, building security measures into his design, and attempting to revise requirements to eliminate those problems he cannot solve. Waiting "until later" to address security seems almost to guarantee the presence of one or more problems that cannot be solved within the existing design and whose solution is expected by the ultimate users of the system.

This paper begins with a brief discussion of the problem of balance in providing security for information systems. Next comes a more specific discussion of the problem of protection in computer and operating system software. The third section discusses what can be characterized as partial software protection measures, and the fourth describes principles for achieving complete software protection.

* The work reported herein was sponsored by the Air Force Electronic Systems Division under Contract F19628-73-C-0001, Project 572R.

Balanced Security

In designing an information system that handles sensitive information, considerations of threat and vulnerability are basic. In this context, the concept of threat refers to the willingness or intent of a hostile agent to access the information. Vulnerability refers to characteristics of the system itself that allow such access to take place. Consideration of accidental damage or access is also required, but can be handled by relatively straightforward thorough practice and seems fundamentally different from the consideration of hostility and malice.

In considering threat and vulnerability, the designer would do well to keep in mind that a rational opponent will attack a system's weakest point. Thus, providing great protection at one point of potential vulnerability may only drive a hostile agent to attack another point of vulnerability slightly less weak than the first. Only if the entire system is protected to about the same extent—if the protection is balanced—can the designer claim to have expended his protection resources in a reasonable manner.

The appropriate measure for the level of system protection is the hostile agent's cost—not the designer's. The next section of this paper discusses the history of secure operating system design efforts in which designers have expended tens of man-years "protecting" systems only to find that their efforts could be undone by a hostile effort of a few man-months. In such cases, designers have presumably assumed that the effort to defeat their protective measures would be roughly proportional to the effort required to implement them. Such assumptions, while comforting, are not a priori valid.

The requirement for balanced protection is, of course, system-wide. Some systems using remote tern.i-

nals have implemented elaborate password and user identification schemes but ignored the requirement for protection of communication lines. For some classes of threat, such designs are perfectly reasonable. But the designer of such a system who asserts that his system is secure because it would take thirty-eight hours (or days or years) to break the password system and who ignores the possibility of achieving the same end with a wiretap and ten minutes' effort does himself and his audience a disservice. A realistic assessment of system-wide vulnerability is required, and this assessment is seldom identical with an assessment of the vulnerability of the last-designed security feature.

It is the concept of balanced protection that motivates dedicating much of the remainder of this paper to software and operating system protection and vulnerability. As users, managers and designers become aware of exposures in such areas as communications, personnel, and procedures, it appears likely that they will implement protection in these areas and drive hostile efforts toward the weaknesses of the operating system software.

The Problem of Software Security

The basic problem of security and protection in today's computer systems is that any program that runs on a computer can assess any information physicaly accessible to the processor, and can retrieve, alter or destroy the information as the programmer wishes. While the statement above may appear to be a radical one, it is amply supported by facts and experience. On numerous occasions, programmers have conducted formal or informal projects aimed at testing the security of operating systems by penetration—by writing programs that obtain access to information without authorization. The author has participated directly in several of these penetration projects and observed the results of others. In each case, the result has been total success for the penetrators. The programmers involved in these efforts have not been "insiders" but simply competent system programmers armed with user and (sometimes) system level documentation for the computer and operating system under test.

Given experience in the penetration of computer systems, one might ask "why not simply modify the operating system programs to correct those flaws that allow the penetration to succeed?" There are two problems that preclude this approach (often referred to as "patching holes") from being effective. The first, a practical problem, is that in many cases operating system or application programs will not work if a hole is patched. Thus, correcting a security flaw may render the computer system inoperative unless a long, costly series of program modifications is made. The second problem, a fundamental one in the field of multilevel computer security, is that of completeness. Even if every hole that allowed a known penetration approach to work were repaired, one still could not consider the resulting operating system secure because a given collection of penetration programs exposes only the holes that those programs exploit. Short of constructing the (astronomically large) set of all possible penetration programs, one can make no statement at all about undiscovered holes or the penetration programs that would exploit them. This problem is compounded at the practical level by the fact that complex and expensive program modifications, intended to patch existing operating system holes, have themselves a significant likelihood of introducting new holes in previously sound areas.

The problem of completeness, as stated above, might lead the reader to rebel and proclaim that completeness is not necessary, that nowhere else is perfect security required—that physical, personnel and even communications security measures have finite probabilities of penetration. One might then say that in a computer it should be similarly possible to accept a degree of security less than a hundred percent. Unfortunately, the usual analogy between operating system security problems and those of physical, personnel or communications systems is not a correct one. If an error in an operating system program allows a penetration program to work, that program will work every time it is executed—typically retrieving without detection any information accessible to the computer. The probability of a successful penetration is then unity; the level of security zero per cent. The likelihood that a hostile agent will write the penetration program is, therefore, the only uncertainty. This likelihood is hard to assess, since it depends on the motivation and competence of the agent. However, experience with penetration tests leads to th conclusion that the penetrator's changes of success are very high. Although concealing the structure and weaknesses of the operating system modifications may seem to obscure the structure and weaknesses of the security controls, such a primitive encoding scheme does not effectively deter penetration; knowledge of the basic processor hardware and standard operating system provides an adequate starting point for the penetrator's efforts.

A final point about the vulnerability of current computer systems concerns the cost of penetration. Most penetration efforts have been completed successfully with very few (perhaps two) man-months of effort. Typically, the bulk of the effort expended is directed toward exploitation—finding information to be retrieved and building programs to retrieve it. Development of the basic approaches that assure successful penetration has usualy required only a man-week or two. In comparison, the effort expended in patching operating system holes is rumored (most agencies that have performed such patches are reluctant to report costs) to be in the tens or hundreds of man-months.

This brief overview of the technical problem of software and operating system security is not intended to portray the problem as a hopeless one. Rather, the section has been written to indicate the nature of the problem and its position in a consideration of balanced security measures and threats. The next two sections discuss partial and complete measures for addressing software security problems.

Partial Measures for Software Security

Designers of information systems that must face security problems are often interested in partial measures that can be introduced at low cost to provide limited protection. The true limits of such measures should be painfuly evident from a reading of the section above, for none has any effect on the ability of a programmer to construct penetrations of the sort discussed there or the cost of doing so.

Auditing

As various computer-related crimes have touched the financial community, interest in computer auditing has increased significantly. Auditing is an approach to detecting an irresponsible action within the "rules" of a system. It will detect a bank teller who, using an online transaction system, makes a "withdrawal" from a customer's account. Similarly, in a time-sharing system, auditing can detect an attempt by a user (successful or not) to log in using another user's password. But auditing cannot detect actions by the agent who does not follow the rules of either system. In the first case, a programmer can add his own unaudited transaction type to alter balances within the bank's master files; in the second, the time-sharing user can log in using his own identity, then constructs a program to access files owned by any other user without using that user's password.

In a system without complete and effective access controls, auditing is of no help in detecting either programmed attack; in a system with such controls it is not necessary, for the attacks wil fail. A system equipped with access controls does require auditing to detect irresponsible actions by authorized individuals. The teller who "plays around" with accounts he can legally access or the user who gives away his password will leave detectable traces in a system with access controls as wel as auditing. However, the value of auditing is indeed limited.

Passwords

Passwords provide a mechanism for assuring that an individual is, with a given probability, who he tells the password processing mechanism he is. For this purpose, they are an appropriate tool. But almost all of the numerous programmers who have penetrated time-sharing systems logged in with passwords and then ignored completely the password assigned to the users whose files they stole or altered. Passwords are only an identification mechanism; they provide no internal protection.

The use of file passwords in some computer systems may seem to contradict the statement above. In fact, however, such passwords merely provide a shorthand for a list naming those individuals authorized to access the file. The price for that shorthand is that a list is complete and closed (one is on the list, or he is not) while the password is open (anyone can guess it). Thus file passwords merely introduce an element of chance in return for compactness of representation. The protection associated with file passwords merely introduce an element of chance in return for compactness of representation. The protection associated with file passwords is that of the operating system that implements them—few indeed are the penetrators who have forced to guess at file passwords.

External Security Computers

A number of proposals have been made for the use of external minicomputers to perform a security control function for a large computer system. The key issue in evaluating such a configuration is the role of the minicomputer. If it provides all of the security controls such a minicomputer can solve the problem of completeness and implement an effective security system [1, 2].[1]

If the external minicomputer merely observes the actions of the main computer to watch for improper actions, or if it shares the role of security controller with the main computer, it can easily be fooled or bypassed by a hostile agent's program on the main processor. In this case, of course, the external minicomputer does not provide effective controls and is of little or no value.

Complete Software Protection Measures

The computer system designer who requires effective protection, and who cannot "lock his system up" to depend on physical security, procedures, and trusted people requires an effective software security control system. The following paragraphs describe briefly the evolution and basis of such systems.

The Computer Security Technology Panel

In 1970, the Air Force Electronics Systems Division (ESD) was asked by the Air Force Data Services Center (AFDSC) to support the development of secure operation for AFDSC's Honeywell 635 computer systems. The 635s operate under control of the standard GCOS III operating system. After a relatively brief period, ESD and MITRE personnel pursuing the development reached conclusions substantially identical to those reported in the previous section—that no set of modifications to GCOS III would render it suitable for secure operation.

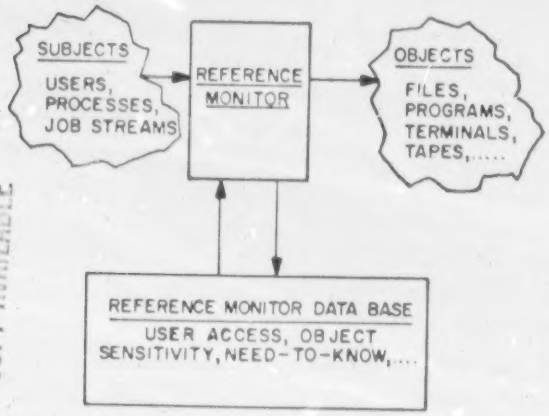
In an attempt to determine the reasons for the difficulty with GCOS III and to identify ways of solving future computer security problems, ESD convened in early 1972, a computer security technology planning study panel. The panel operated under a contract from ESD to James P. Anderson and Company and was tasked to prepare a development plan representing a coherent approach to attacking the problems of multilevel computer security. The panel's report [3] identified the problem of completeness and recognized the

[1] Figures in brackets indicate the literature references at the end of this paper.

futility of "patching holes" in existing operating systems. The technical approach recommended by the panel was "to start with a statement of an ideal system, a model, and to refine and move the statement through various levels of design into the mechanisms that implement the model system" [1]. The following subsection discusses the characteristics of the "ideal system" as proposed by the panel and detailed by subsequent efforts.

The Reference Monitor

The basic component of the ideal system proposed by the security technology panel is the reference monitor—a hardware-software mechanism that controls the access of subjects (active system elements) to objects (units of information) within the computer system. Figure 1 presents a schematic diagram of the relation among subjects, objects, reference monitor, and reference monitor authorization data base. The figure gives examples of typical subjects, objects, and data base items.



BEST COPY AVAILABLE

FIGURE 1. *Reference Monitor.*

In operation, the reference monitor allows or forbids access by subjects to objects, making its decisions on the basis of subject identity, object identity, and security parameters of the subject and object. The reference monitor both mechanizes the desired access rules and assures that they are enforced within the computer.

The security technology panel stated that a reference monitor must meet the following three requirements in order to provide the basis for a secure computer system:

a. Completeness—the reference monitor must be invoked on every access by a subject to an object;

b. Isolation—the reference monitor and its data base must be protected from unauthorized alteration;

c. Certifiability—the reference monitor must be small, simple and understandable so that it can be tested and verified to perform its functions properly.

Both the requirement for completeness and that for certifiability demand that the reference monitor include hardware as well as software—the former because software validation of every access by a subject to an object would add intolerable complexity and overhead to the reference monitor, the latter because certain hardware architectures preclude the construction of a simple understandable operating system. The software portion of the reference monitor has been called the "security kernel."

Recognizing the importance to achieving computer security of the ideal model of a reference monitor, ESD initiated the development of a mathematical model of computer security. Preliminary efforts were performed at ESD [5] and the initial model development was completed by the MITRE Corporation. A later modeling effort using an alternate approach has been pursued in parallel with the MITRE work by Case Western Reserve University [6].

The MITRE model [7] represents a secure computer system as a finite-state mechanism that makes explicit transitions from one security state to the next. The model specifies rules that define formally the conditions under which a transition from state to state may occur. The rules are proven to allow only transitions that preserve the security of information in the system. A significant property of the model is that all but trusted programs are restricted from writing information less sensitive than they read. The restriction prevents information obtained at the higher level of sensitivity from being transferred to a lower level where it can be accessed illegally. This property eliminates the need to certify that all programs such as editors and utility routines do not act as "Trojan Horses" [8] and downgrade classified information.

The finite-state model specifies the secure operation of a system composed of subjects and objects. A security kernel must implement representations of both the rules of the model and the subjects and objects these rules control. The implementation of subjects and objects is constrained by the hardware on which the kernel operates. If the hardware does not facilitate the simple implementation of subjects and objects, the third of the panel's requirements for a reference monitor will not be met. The panel recognized this fact and recommended for secure computer systems the use of descriptor-driven[2] processors that implement segmented memories. With such processors, the objects of the model can correspond to the segments supported by the hardware. A properly organized segmented memory merges primary (core) and secondary storage management functions, eliminating from security consideration

[2] A descriptor-driven processor is one whose hardware interprets each "virtual" address issued by a program in terms of a set of descriptors that specify the real physical address and permitted access modes (e.g., read, write, execute) to be associated with every possible "virtual" address.

any separate, complex, and security-related "file system." Further, the subjects of the model correspond to processes (address space-processor state pairs) supported director by a descriptor-driven processor.

The security kernel defined by the model and implemented on descriptor-driven hardware is a simple software mechanism that implements only the security rules, subjects, and objects. It does not provide the full facilities of an operating system; it could not do so without developing so much complexity that it would no longer be a security kernel. Instead, the complex functions required of an operating system are provided by programs external to and controlled by the kernel. These functions can be arbitrarily complex but are not security related. However, some may be sensitive in terms of assuring the smooth operation of the computer system. For example, a typical operating system (not kernel) function like a scheduling algorithm cannot compromise information, but it can slow service to users.

To assure that user programs can be separated from (and kept from interfering with) such sensitive programs, the MITRE development efforts in multi-level security have identified the need for hardware with at least three separate domains of execution (states of program privilege). Of these, one can be allocated to th kernel, the second to the operating system, and the third to user programs. The kernel can easily protect the operating system from user programs and, because of the organization of the hardware, the transitions from one domain to another can be rapid and efficient.

In summary, this subsection has identified the concepts of a security kernel and discussed a model of a kernel that represents the secure operation of an ideal reference monitor. It has also mentioned the requirement that the kernel implement subjects and objects, and pointed out that their simple implementation hinges on the architecture of the computer that the kernel controls. In particular, a secure computer is required to provide a segmented memory and at least three processor domains. The above discussion has not been explicit about the transition from the model to programs that implement a kernel on specific hardware. A discussion of that transition is included in [9].

Summary

This paper has discussed some of the security considerations involved in designing a computer-based information system. It has emphasized the software problems presented by such systems, mainly for the reasons that the costs of effecting a software penetration are not great and that many designers seem unaware of the seriousness of software penetration problems.

References

[1] Lipner, S. B., A Minicomputer Security Control System, MTP-151, The MITRE Corporation, Bedford, Massachusetts.

[2] Bisbey, R., II, and Popek, G. J., Encapsulation: An Approach to Operating System Security, USC/Information Sciences Institute, Marina del Ray, California, October 1973.

[3] Anderson, James P., Computer Security Technology Planning Study, James P. Anderson and Company, ESD-TR-73-51, Vol. I, Fort Washington, Pennsylvania.

[4] Ibid, pp. iv.

[5] Schell, R., Downey, P., Popek, G., Preliminary Notes on the Design of a Secure Military Computer System, MCI-73-1, January 1973, USAF Electronic Systems Division, L. G. Hanscom Field, Bedford, Massachusetts.

[6] Walter, K. G., et al., Primitive Models for Computer Security, ESD-TR-74-117, Case Western Reserve University, Cleveland, Ohio, January 1974.

[7] Bell, D., and LaPadula, L., Secure Computer Systems, ESD-TR-73-278, Vol. I, II, III, The MITRE Corporation, Bedford, Massachusetts.

[8] Branstad, D., Privacy and protection in operating systems, Computer, V. 6, No. 1, January 1973.

[9] ESD 1973 Computer Security Developments, MCI-74-1, January 1974, USAF Electronic Systems Division, L. G. Hanscom Field, Bedford, Massachusetts.

AUDITING CURRENT SYSTEMS

Donn B. Parker

Stanford Research Institute, Menlo Park, California 94025

To provide an idea or a sample of the kind of actions that must be taken to develop an accepted practices approach to this important aspect of computer security and privacy, I will discuss some of the problems concerning the safety of our organizations that are dedicated to the use of computers. From the point of view of the auditing function, I will indicate what the problems are, what the state of the art is in EDP auditing, and some of the specific problems and solutions.

We find that unintentional acts, failures that result in losses, white-collar crime, and other abuses have always occurred in manual systems and environments in organizations. Computer technology, however, is automating the previous manual systems and taking over these environments. Therefore, if losses are to continue, they must continue in the new systems and environments that computer technology creates. Unfortunately, computer technology has developed for the most part with the assumption of benign environments rather than the hostile environments actually emerging as proliferation of computers into sensitive social, government, and business functions continues. Of course, we are referring to the same old errors, omissions, floods, fires, explosions, frauds, thefts, extortions, vandalisms, larceny, and compromises of personal rights that have always occurred. However not only automation in the environments, but also the occupations of people causing and perpetrating such infractions have changed. The methods, processes, and time scales by which they occur have changed; the forms of assets and losses, the rates of incidence, and size of losses have changed with advancing computer tech-

nology. This is confounding the victims, the preventors, the detectors, the recoverers, the regulators, and the lawmakers. The basic kinds of problems facing organizations are essentially the same, but the methods and the environment have created a very new problem. As advancing computer technology accelerates this change, the elements necessary to preserve order, safety, and the welfare of people and organizations lag behind. Our initial studies of actual experience validate such trends. Almost 200 cases of reported computer abuse are recorded. Some of these cases were verified and a few of them were investigated in depth; for the first time they provided more than just theoretical or presumptive evidence of this situation. These cases were discovered mostly by accident rather than with purposeful methods.

Now the solutions and the control of these problems concern the safe operation of organizations. Traditionally, this is a concern of auditors; moreover, it is important to continue to include the auditors in any attempts at solution and control. The solutions to the problems identified are coming from legislative action, from the theoretical and empirical research, and from the development activities being documented in this conference. In addition, one of the major areas of solution and control activities must be auditing.

Heretofore, auditing has been associated with accounting activities. Auditing however is more broadly defined as the left arm of management—it ensures compliance with all policy integrity and correctness of business records. At this time as computers take over the environments of traditional auditing new demands are placed on auditing functions. For example, the Institute of Internal Auditors, the American Institute of Certified Public Accountants, the National Association of Accounting, other groups such as the EDP Auditors Association, and government bodies such as various state insurance commissions are striving to develop new methods in auditing to match the advancement of the systems that they must audit.

A new specialization currently called EDP auditing has emerged in the last several years. Banks have probably led the way in this specialty. Several large banks have a ratio of one EDP auditor for every ten to thirty programmers; some large banks have as many as sixty to one hundred EDP auditors. The EDP auditors' charters are expanding to include accountability for computer-resource usage and data access. This was indicated in the proceedings of the first conference here at the National Bureau of Standards. The diverse functions now required of auditors in EDP environments necessitate further specialization for in-depth penetration into all aspects of protecting organizations in EDP environments. The specific areas of specialty include physical security, operational security—including recovery and backup—application analysis and programming, systems programming, and electronic engineering. This implies a team approach to auditing to achieve the necessary depth of expertise in these diverse areas. We find organizationally that the line functions implement and operate security activities and controls. Whereas auditors establish the criteria for controls and security and then monitor and report on the performance; they normally report to a high enough level to be independent from the line functions they audit. In the future, the term EDP audit will probably become obsolete because all auditors will essentially become EDP-oriented, but their organizations will have specialists in the various subject areas that I have identified.

Auditing methods in advanced EDP environments are in a state of confusion. They have been developed on an ad hoc basis and are unrelated from organization to organization, with no unifying technology beyond dealing with the most rudimentary batch-operated systems. In fact, a considerable lack of awareness exists among many auditors as to the vulnerabilities concerned with computers. An auditor today generally believes that he can remove his audit program on punched cards from his locked drawer, take it to the computer room, observe it reading into the computer, observe the source files on tape or disk being mounted, watch the lights blink and the report come out of the printer and be confident that his program is correct. It was correctly run, and it produced correct output. He is unaware that the systems programmers, operators, or maintenance engineers could have deceived him without his knowledge. Not generally realized, however, is that today the best an auditor can do is contain or isolate the problem area. Unfortunately, he usually is unaware that the problem exists, and lacks know-how to control it. Historically, the auditor has handled visible records and processes. In the computer environment, he must accept on faith from the programmers, operators, and engineers that the computer is storing, controlling, and processing data correctly within the system. This violates basic concepts of auditing.

To solve these problems, we must develop and document accepted good practices for auditors in EDP environments. Let me provide examples of some of the specific problems and solutions to these problems and thereby indicate the range and nature of the practices that must be established.

In one computer abuse case that we investigated, a programmer allegedly embezzled through a computer even though a record of the act was also produced in the exception reports. He relied on the fact that no one bothered to look at the voluminous exception reporting output listings. He was successful in his embezzlement primarily because he was able to hide his act in this fashion. Humans should not be expected to look at voluminous exception reports produced daily by computers; rather, this is a job ideally suited for computers to reduce the voluminous data to a possible one page analysis.

Consider another aspect of the problem that is often overlooked. Vulnerability is the highest at times when irregular operations in a computing facility may be caused by various failures, unusual work loads, or system changes. I have documented several cases of computer abuse that have occurred at these most vulnerable times. Extraordinary operational procedures should be established in advance and should be practiced to facilitate operation during these periods of high vulnerability when suspicion of possible damaging

activities is high. For example, a common practice is to store only one copy of sensitive files and programs in remote backup facilities. After an emergency occurs and the backup facilities have been used, these files are returned to the computing facility. The computing facility is now in an even more vulnerable position because the remotely stored backup has been removed, and the only copies of the sensitive files and programs are now in the computing center—which is in its most vulnerable state. One possible, obvious solution is to remotely store two copies of sensitive files and programs and to have auditor verification that they are updated and useful. These periods of extraordinary activities also have a positive aspect. Acts or events resulting in losses are sometimes discovered during unusual operational periods that would not have been discovered otherwise. Several cases that I have documented support this. Therefore, change or extraordinary operational conditions properly controlled can be an effective detection mechanism.

Turning to another area of application program controls, we find that data validation is usually performed in application programs at the point in time when data are entered into the system. A suggestion has been made that this should be changed so that the general rule would indicate that validation should be performed within the computer in proximity to the time and place of use or before a process-termination test—whichever occurs first.

For example, extra protection is afforded for labor hours input to payroll applications if the in-range validation is performed in the pay calculation process rather than during input to the computer. This is especially true in an integrated system where many opportunities could exist for programmed, unauthorized alteration between these processes.

Auditing also has a role to play in expected new laws to come from the current privacy legislation activities.

Detection and monitoring of noncompliance with privacy and security practice and policy in computer systems will be the auditors responsibility. This is an important constraint on how security is designed and implemented. The basic elements found in most of this legislation consist of defining information jurisdictions, regulation, licensing or registration, sanctions, full disclosure, due process, and protection of information. Assurance of compliance with these anticipated laws falls within the responsibility of auditors within organizations affected by the laws. Surely, the auditors should be consulted concerning their ability to prove compliance with the full disclosure, due process, and protection elements and to determine the definition of adequate protection in their organizational contexts.

Since auditors are removed from the line functions of the designers, implementers, and operators of security functions, they can examine and judge the consistency of measures taken and the consistency of resources expended for security. They can observe that physical security measures implemented by the security department are consistent with the security measures adopted by the computer operations department. For example, auditors can see the common situations where expensive man-traps are installed to control physical access, but the operators on second shift prop the emergency exit door open with a box of cards because it is the most direct route to the coffee machine. Or consider the cases where extensive programming is done to provide secure access control to commercial timesharing systems even though a known bug that allows free access to the entire system still exists in the Fortran compiler. In one particular case, even though one customer was caught penetrating the system in this fashion, the reason the bug remained unfixed was that no other customers had ever been found using that method of penetration.

Again, consistency is the key to the most effective application of resources to security. Auditors should ensure that the simple, inexpensive, but effective security measures should be taken before they worry about more elaborate measures to protect other, but equally vulnerable situations. I have several documented cases that illustrate this point. For example, very few organizations take the trouble to label their programs to identify the ownership. This requires a very small expenditure of effort and resources, yet has a very valuable effect in programmers attitudes towards the ownership of the programs they produce and has an added value where programs are involved in matters of litigation. In another example, we find that timesharing systems rarely provide the equivalent of "NO TRESPASSING" or "DO NOT ENTER" signs within their systems. Therefore, the users of these systems are given no rules concerning the kinds of activities permitted once they have achieved legitimate access to timesharing systems. As another example, I find that very few employees in data processing organizations understand the extent of the trust placed in theim and their security responsibilities. I suggest that this situation can be improved considerably by a requirement that all EDP employees in sensitive positions read a document explaining their trusts and responsibilities and sign a statement that they have read these regulations at least once each year.

Auditing includes assurance that emergency measures work by conducting tests. In one case, the under floor CO_2 fire extinguishing system had never been tested, but it was activated once by accident. It was then found that because the CO_2 was heavier than air, it leaked down to the floor below and almost killed several employees there. This is another example of the continuing need for broad examination of security measures and the testing of these measures by an independent organization, either internal to the organization or by external consulting services. The ultimate goal of security and protection of confidentiality is to reduce to a minimum the number of people in whom we must put complete trust and faith. The auditors have traditionally been these people in our organizations. Efforts towards security in computer systems and environments should continue this tradition. We must not forget the auditing functions in the development or privacy and security in computer systems.

OPEN FORUM REMARKS

THE MEDICAL PATIENT'S RIGHT TO PRIVACY

Lois A. Bowden

American Hospital Association, 840 North Lake Shore Drive, Chicago, Illinois 60611

Within the broad spectrum of records that are maintained on individuals, the medical record is unique and its special characteristics require our thoughtful consideration. The American Hospital Association has long recognized these special characteristics and requirements for protection of the patient's right to privacy.

The primary purpose of the medical record is to document the course of the patient's illness and treatment. As such, it serves as a basis for the planning and evaluation of individual patient care and for communication between the physician and other professionals contributing to the patient's care. And although medicolegal applications, research, teaching, data collection, and validation of insurance claims are extremely important uses of the medical record, they are secondary.

As the hospital medical record is being subjected to greater demands for its use and for the release of medical information, it is becoming increasingly difficult to maintain the confidentiality of patient information. Financial, legal, adminstratve, educational, research, and audit requirements are factors that contribute to the complexity of preserving confidentiality; and the original concept of the medical record as a tool with which the practitioner manages patient care often is lost in proposals for the acquisition of patient data for nonpatient-care usage.

In releasing information from patient records, the many questions that arise that are not covered by statute, court decision, or regulation are determined by hospital policy and the judgment exercised thereunder. Therefore, the Association has provided guidelines and general principles for information disclosure.

Recent Association publications include the manual, *Hospital Medical Records: Guidelines for Their Use and Release of Medical Information* (published in 1972), the *Statement Against the Use of the Social Security Number for Patient Identification* (1973), and the *Statement on Health Data Systems* (1973). In further recogniton of the special characteristics and requirements of the patient's medical record as it affects the patient's rights of privacy, the American Hospital Association included within its *Statement on a Patient's Bill of Rights* (adopted February 1973) the following:

> "The patient has the right to every consideration of his privacy concerning his own medical care program. Case discussions, consultation, examination, and treatment are confidential and should be conducted discreetly. Those not directly involved in his care must have the permission of the patient to be present.
>
> "The patient has the right to expect that all communications and records pertaining to his care should be treated as confidential."

Traditionally the patient's right to privacy has been protected through the use of his written authorization. Technically the patient's written consent governs the release of information concerning his illness. Realistically the various previously-mentioned pressures for such release have diminished the significance of written consents.

In view of this tradition and of new developments affecting the use of medical records, the Association's Board of Trustees voted in November 1972 to request that a thorough exploration of the problem of confidentiality of patient records in light of recent legislative enactments concerning federal health care programs be undertaken.

In response to this charge and in light of the recommentadions on safeguard requirements for administrative personal data systems, outlined in *Records, Computers and the Rights of Citizens*, the American Hospital Association's Committee on Medical Records has undertaken to examine the appropriate definition, specifications, and limitations for a properly executed authorization for release of information—so as to provide the right information to the right person at the right time.

In addition, this committee has expressed grave concerns with regard to the unknown and unauthorized secondary release of medical information by persons and organizations, both public and private.

This committee would appeal that legislation created in the interest of third party payment and other secondary uses of the record, also provide for the patient's right to privacy, thereby encouraging the use of medical information that is not personally identifiable wherever possible.

It is the sincere hope of the American Hospital Association that all of these activities and those of others concerned with security of information systems will lead us to a workable solution of these problems and concerns that will satisfy the legitimate need for medical information, while protecting the rights of confidentiality of the patients served and preserving the integrity of the patient's medical record to adequately fulfill its primary function: the documentation of patient care and treatment.

OPEN FORUM REMARKS
CONFIDENTIALITY OF THE MEDICAL RECORD

Margaret C. Beard

American Medical Record Association, 875 N. Michigan Ave., Chicago, Illinois 60611

Economic and social issues, together with technological advances, have resulted in an erosion of the confidential relationship traditionally existing between patient and health care professional. The proliferation of health insurance programs has been accompanied by an ever increasing number of requests for information from patient health records in substantiating claims for payment. At the same time, a growing emphasis on accountability has resulted in further demands for patient health information for medical care evaluation, including utilization review, which has caused a tremendous growth in the number of automated data storage and retieval systems for information management.

The primary purpose of the medical record is to document the course of the patient's health care and to provide a medium of communication among direct care professionals for current and future patient care. Unless the patient can feel assured that the highly sensitive and personal information he shares with health care professionals will remain confidential, he may withhold information critical to his treatment, thereby diminishing the quality of the care provided him.

The American Medical Record Association (AMRA) recognizes the need for patient health information in providing a sound basis both for substantiating claims and for conducting medical care evaluation. Through this statement, however, AMRA reaffirms the patient's right to privacy in relation to his medical record. While the patient does not have the property right to his record, he does have the protected right of information. Therefore, subject to applicable legal provisions, release of any individually-identifiable medical information for any purpose other than patient care must be done only with the express informed authorization of the patient or his legal agent.

With respect to this right of privacy, AMRA endorses the development of legislative and regulatory activities to: (1) protect the patient from invasion of privacy as a result of indiscriminate and unauthorized access to confidential health information and (2) assure appropriate usage of medical information once it is disseminated by authorized persons.

Further, AMRA recommends greater emphasis on the patient's right to privacy by health care institutions throuhg the establishment of written policies for the release of informaiton, together with active educational programs for all staff personnel to enforce these policies.

OPEN FORUM REMARKS
MODEL LEGISLATION

Brian Backus

Ohio Department of Administrative Services
30 East Broad Street, Columbus, Ohio 43215

As day-to-day guardians of large volumes of personalized information both in automated and manual systems, we in state and local government feel that a great measure of responsibility for the protection of this kind of information rests with us. As operators of government information centers we believe that we stand in a position where we can be useful in the design and implementation of procedures for the protection of the privacy of personal information.

To this end, two organizations representing all 50 states and many municipal governments have been studying the problem of legislation in this area. They are NASIS (National Association of State Information Systems and G-MIS (Government Management Information Sciences). Their work was based on research done for the SAFE (Secure and Automated Facility Environment) in the State of Illinois. The fruits of this effort are now being realized. It is model legislation for state governments covering the regulation of personal information in the possession of the states. With this document we believe that we have come a long way towards a practical means of dealing with the problems of privacy and towards protection of the individual. We have also addressed the management and regulatory needs of government data centers.

The significant features of this legislation are:

1. It regulates any personal data, not just data in automated systems. It applies only to data in the possession of state and local governments, but can be expanded to cover the private sector as well.

2. It defines the individual's rights to be protected:
   a. the individual can request and be notified if a file contains personal information about him. In most cases, he can see the contents of such files.
   b. On his request inaccurate or incomplete data is to be corrected or amended.
   c. The individual is to be free from:
      —uses of data outside the purposes of the system
      —continued collection and storage of obsolete information
      —use of information whose accuracy cannot be verified
      —coercion to give information about himself.
   d. The individual has a right to know how information concerning himself is used.

3. It creates a regulatory body, an Information Practices Board with a staff. The duties of the Board include the promulgation of administrative regulation for organizations which own personal data to insure security and confidentiality of data. The Board also would conduct investigations of questions which arise concerning the law and regulations and lend flexibility in situations where strict adherence may not be merited. It would hear appeals on decisions regarding privacy by state and local agencies and data processing authorities.

4. It gives the Board the power to establish local boards to regulate data at that level.

Those interested in obtaining a copy of the finished document may write to:

G-MIS
138 E. Court St.
Cincinnati, Ohio 15202.

OPEN FORUM REMARKS ON INFORMATION FILES AND PEOPLE

Mark P. Kriger

Harvard University, 520 Gund Hall, Cambridge, Massachusetts 02138

To my knowledge at the present there are only two universities in this nation which currently have courses on the subject of "Privacy and Security in Computer Systems." I want to thank you in helping me to plan teaching a course on this subject. The many conflicting and cooperative viewpoints represented here at this conference have been most valuable.

In the following few minutes I would like to share with you several ideas which have not been mentioned and which merit consideration. The first of these is the notion of "information flashpoint." It is clear that the advent of large-scale computer systems results in a larger quantity of information available. However, as computer networks, and especially, information processing utilities come of age there is a possibility of qualitative changes in the information as files become merged or easily accessible from a terminal. For example, when we bring together unclassified files containing codes and data and a simple algorithm for analysis it is often possible for that information then to become classified in nature.

A second item which computer scientists, managers, and public policymakers would do well to guard against woud be the growing trend of what might be termed "information pollution." If we do not take measures to constantly eliminate what is not needed in files then we will have information systems so cluttered with meaningless or irrelevant data that the information which is required will be buried and less usable. Insuring the clarity and accuracy of information is also related to this notion of information pollution.

Thirdly, we might begin to look at an individual's personal space as being extended by and related to his information space. Before the advent of large information files a person's private space was pretty much equivalent to his home and place of work. When we increase the information available about a person we increase what we might term his "information space," which is to say, that his personal identity in an information sense has been increased and even redefined.

In closing, I would like to share with you the words of a Chinese sage named Lao Tse, who lived in fourth century B.C. China. In his "Treatise on Response and Retribution," he wrote:

> "If a man's heart be awakened to the good, though the good be not yet accomplished, good spirits are already following him.
>
> If a man's heart be awakened to evil, though evil be not yet accomplished, evil spirits are already following him."

Translating this advice into the present computer age, this is to state that we have a need for men and women of good intent in the design, maintenance, and updating of information files, manual or computerized. Let us remember that the information files which we are creating and maintaining are about real people whom we have in many cases not met and never will meet. Nonetheless, we are continually defining and extending the information space about these people.

OPEN FORUM REMARKS
THE NEED FOR PRIVACY LEGISLATION

Robert H. Long

Bank Administration Institute,* P.O. Box 500, Park Ridge, Illinois 60068

I have heard no evidence presented that indicates that the use of automated personal data systems has created increased invasions of privacy or breaches of confidentiality. In fact, some speakers have stated that no such evidence exists. We have heard only that there is a "fear" that such may be the case.

Based upon this unsubstantiated fear, it appears that we are considering legislation that will force registration and perhaps monitoring of automated personal data systems.

It does not appear that the end justifies the means. It appears that we are placing a financial burden on the taxpayer and the businessman simply because we are afraid something might happen.

Furthermore, periodic reporting of the existence of an automated data file will not accomplish any practical purpose. Flooding a newspaper with 15 or 20 million data file announcements a year will not increase anyone's awareness of who has a file on him. Who has time to read the announcements or to investigate them?

Existence announcements or registration will no more prevent data misuse than registration of automobiles has prevented their misuse. In fact, such registration laws:

1. Are impractical and unenforceable on a broad scale. Therefore they are unwise, because impractical and unenforceable laws weaken respect for all law.

2. Penalize automated data file owners for what they *can* do, not for what they *do*. There is no evidence to suggest that such presumption of guilt is justified.

3. Make it possible for the government (since only it has the massive resources required) to create a complete central file on all citizens. Thus, registration would increase the potential for reducing individual privacy. There is no demonstrated need for such government power and I object to making such power possible "in the name of protection of privacy."

Several speakers have voiced the idea that "the individual owns data about himself." I believe this is a fallacious and unusable concept.

I can create all kinds of information about an individual, based on my own observation. He does not own this information. It is mine. If I use it to harm him, then I alone am responsible and he should have a ready and rapid method of redress. But he does not own the information any more than he owns the picture that I may take of him. Information belongs to the creator or the collector and he alone must be held responsible for its accuracy and its use.

The way to protect privacy and confidentiality is to improve the procedures of redress, not to attempt to monitor or control every personal data file at a governmental level.

I think that we should improve redress procedures. We should make it easier to trace erroneous data to its source. We should increase the personal data file owners' awareness of their responsibility. But the rules should apply to all personal data, whether automated or non-automated. With the development of mini-computers, automated personal data files will soon include Christmas card lists, YMCA swimming teams and the neighborhood Fourth-of-July picnic list. No practical purpose would be served by requiring public notification that such files were being set up.

Finally, we may find that a public notice requirement will grow into a requirement for licensing, and that licensing will pave the way for data file taxation. Should we start down such a pathway in the absence of any evidence that the misuse of data is growing? Perhaps misuse is diminishing because of automation. Let's get some facts, let's not legislate out of fear.

The supposed cure may be worse than the presumed illness.

* The views expressed are those of the author and not necessarily those of BAI or the banking industry.

OPEN FORUM REMARKS

THE ADMINISTRATIVE BURDENS OF PRIVACY LEGISLATION

Edwin I. Golding

Office of Law Enforcement, Dept. of Treasury, Washington, D.C. 20220

When one discusses computer security, data confidentiality and privacy, there should be a general awareness that these items operate within a system of interacting elements. As a consequence, one should anticipate how the implementation of controls on any one element of the system affects the remaining elements. For instance, there has been considerable time spent at this conference in order to describe the problems and useful solutions for the major elements involved; that is, for computer system hardware manufacturers, software generators, service centers and their users. We have not, however, given equal emphasis to probably the most important element of the system; that is, the individuals on whom the data is collected especially when they become an active part of the system per se and query agencies, organizations, etc., to find out not only what files there is data on them but also the information content of such files. The enormity of problems that could result in both administrative and dollar requirements should be clearly understood before there is a broad institution of search and query by the general public. This is necessary in order to provide an adequate system to handle inquiries that could result.

For instance, let us hypothesize that 2 percent of the population suddenly makes inquiries and each inquiry takes 10 minutes to process fully (i.e., search files, make computer runs, prepare correspondence, etc.).

Letting E = Man-years of effort required to process inquiries by individuals with respect to what data in what files effects them

Then: $$E = \frac{P_i \cdot \%_i \cdot t_i}{K}$$

Where: P_i = Population size = 200 million
$\%_i$ = Percent of population making an inquiry = 2%
t_i = Time required to process an inquiry = 10 minutes
K = # of man-hours/years (8 hour/day, 40 hour/week)

Then: $E = 333$ man-years

But suppose that instead of 2 percent of the population, 10 percent of the population, i.e., 20 million, are interested in making an inquiry, then:

$$E = 333 \times 5 = 1{,}665 \text{ man-years.}$$

Furthermore, suppose that 10 minutes to process inquiries is too conservative, instead it takes 60 minutes; so that:

$$E = 333 \times 5 \times 6 = 10{,}000 \text{ man-years.}$$

If this workload of required effort was distributed say to 50 locations, one for approximately each state, then the Effort (E_s) required at each location might be:

$$E_s = \frac{10{,}000}{50} = 200 \text{ man-years.}$$

The 10,000 man-years of effort required at a central location or the 200 man-years at each of 50 locations are just possible estimates for initial requests. One can assign his own cost factor and calculate the dollar value for the man-years estimated. In addition, one should consider that there are always follow-up requests, reprogramming of computer software instruction, lengthier searches, etc., and as a result the estimates could be changed depending on what percent factor is used to estimate the effect of such action.

Again, the purpose of the above is not to down play the rights of an individual with respect to information privacy and confidentiality but to make us aware of the impact!

There are solutions. Some are extreme, like purging every file and starting all over with affidavits showing an individual's condescendence to have files structured with data specifically on him. A less extreme situation could be the structuring of particular data inventories similar to that used by the Civil Service in their Executive Inventory files.

In summary, before any laws are enacted, the preceding calculations seem to indicate that in depth consitderation should be given to coping with the administrative burdens that could be created in order to carry out the law. They could be horrendous.

Thank you.

CLOSING REMARKS

Ruth M. Davis
Director, Institute for Computer Sciences and Technology
National Bureau of Standards, Washington, D.C. 20234

Ladies and Gentlemen: This marks the conclusion of a two-part series of Conferences which started last November. We sponsored these Conferences as part of our assigned task of resolving some of the problems of data confidentiality and computer security. We have taken this responsibility rather seriously, as have you. There has been, for example, a total attendance of around 850 between the two Conferences; this indicates widespread interest and concern for the "Privacy" issue.

We very definitely intend to carry out what we promised at the first Conference. As you remember, the first Conference was aimed principally at identifying the needs and the problems of government in assuring the confidentiality of data in automated systems. We have already published a summary of that Conference which has been distributed to all attendees and is available to everyone as an NBS publication. We have attempted to use the second Conference as a return engagement platform for anybody—any organization or any individual—who wanted to provide views on actions that might be taken. We have representatives here these last two days from Congress, from State legislative bodies, from professional associations and societies, from the legal community, from trade associations, individual computer and consulting companies and, of course, a number of private individuals. We are going to publish all papers presented at this Conference.

We also promised that we would make sure that all actions, recommendations, views and concensuses that were generated from these two Conferences would get into the hands of the people who were making or influencing policy. We believed, and you verified it, that this included Congress, the Executive Branch of the Government, the court system, State and local governments, and the computer industry as well as related industries. We intend to do as we promised. For example, a letter has been prepared for Vice President Ford, who has just been designated by the President to chair the Domestic Council Committee on Privacy, which promises that the results of these two Conferences will be given to him within ten days. We will also convey this information to the Congressional committees that are holding hearings. You will recall that one of the comments made here today was the lack of good technical input to these hearings. We want to begin to remedy this by providing the best of what was said at these Conferences and any arrived-at consensus.

In this regard, I really have been very much encouraged by the kinds of statements made today by representatives of institutions in our society, such as the American Medical Records Association, American Hospital Association, the Bank Administration Institute, MIT, Harvard, and some government agencies. This is an excellent way to get your opinions known; and, we're delighted to make them available to people who will make use of them.

Where we have specific responsibilities and authorities in the Department of Commerce, it's even easier to carry out our commitments to you. Let me remind you of some of these responsibilities. We have the responsibility for developing standards which impinge on all Federal information processing activities. These standards are mandatory and can provide a tremendous leverage for action since the Federal Government is still the single largest computer customer in the country and has the responsibility for protecting the public's rights, such as privacy. We also have the responsibility within the Government for marshalling and monitoring the Federal Government's activities in the voluntary standards efforts sponsored within the private sector. We must assess the adequacy of Federal R&D in computer sciences and technology including Federal R&D in computer security and privacy. We have the responsibility for providing to GSA and OMB the technical basis for their policies on computer utilization. The Secretary of Commerce, for example, is offering the same assistance to Vice President Ford and his Committee on Privacy. Being in the Department of Commerce, we serve as a liaison with industry and have the responsibility, as related to computers, for providing the proper environment for commerce and industry.

We do not have major responsibilities in the privacy area other than influencing what's done in making privacy policy and in making sure that we don't trip ourselves up as we try to adhere simultaneously to the need for privacy, freedom of information and integrity of information.

These Conferences have suggested a wide spectrum of actions to ease the problems of data confidentiality and computer security. Some of them we can do ourselves and some we're going to recommend be done by other authorities. The spectrum is too broad to do anything at this time except give you a few examples.

It looks as if it is going to be just as important as we had initially thought to get cohesiveness in the legislative and judicial comments concerned with uniform State laws to get some uniformity in the State laws. We're also going to try to get better technical input to Congressional committees. Congressman Koch said it has become very clear that this needs to happen.

Another area, for example, that we have not touched on extensively but which has come up through default, is the education of everyone concerning privacy. We haven't really educated ourselves enough and certainly have not educated the public either. The American Civil Liberties Union has a publication and reports that come out on a regular basis on privacy. There is obviously a need for us in the Government to provide more

education now in this area than we have been able to do.

We want to and can engage more directly in such activities as pointing out problems of the private sector. We don't believe there is much incentive for industry to put their own funds into R&D and to invest in good, safe, secure systems when those systems are going to be more expensive than the ones that we now use, unless the Government requires security safeguards for individual privacy. So we think there is an absolute need for the Government to stimulate R&D in the private sector through the development of standards, the development of legislation and the development of requirements for safeguards. Otherwise, there is no reason for industry to do more than it has already.

It's more fun to tackle the exotic technological aspects of the problem, but there is also a great need—you heard about it this afternoon and yesterday—for good administrative security. There is an administrative security handbook that will be published next month by the National Bureau of Standards. GSA intends to issue it as a suggested format for Government managers. There is also an executive guide to security that will be coming out soon intended to help executives plan and evaluate their security measures. Finally, I think it is incumbent upon us to recommend that the R&D programs that are underway now and are good—those of ARPA, those of NSF, and other Government agencies—be continued and expanded. And the Government agencies that are not performing R&D in this area, but should be, should be encouraged to become active and have this justified in their budget. This is where the Department of Commerce and, particularly, the National Bureau of Standards, acts as an *amicus curiae* to support this kind of R&D by other Government agencies. We would like to think that in our role as standards-maker we could rely on voluntary standards, and maybe we can. But when the rights of citizens and public protection are involved, one may need mandatory standards. Some combination, therefore, of voluntary and mandatory standards is going to be what we will see in the near future.

Other areas for action include better individual identification. The President's message cites the rights of citizens to inspect and to be able to correct their records. This is not security; this is the opposite. It requires good administrative procedures, good data base management, good validation of software, and good audit procedures.

All of these measures add up to an amount of money for which we do not have good estimates. One thing that is sure is that the problem is difficult and complex. When you have a public good, such as privacy, the problem of "who pays for it" has not yet been determined. You have identified the complexities far better than I can. I have already mentioned that we have to provide simultaneously for the freedom of information, privacy of individuals, and integrity of information. We have demonstrated these last couple of days that the total assurance of what I call simplistic individual privacy is difficult, if not impossible, to achieve. It is compounded by the need to assure the privacy of individual suppliers and users of information as well as the privacy of these people who are the subject of information. But I think, happily, that we are now entering the productive stage in computer security, data confidentiality and individual privacy. We now talk rationally and reasonably. We have heard people give very thoughtful and very deliberate approaches to the problem. I see no reason why these should be withheld from policymakers, from the new Committee on Privacy, or from the Congress. We will make every attempt to get these views to all of those people to help them carry out their responsibilities.

Meanwhile, we want to thank you, the speakers and those of you that have participated, for your interest and contributions. If you want a good definition of productivity, I would suggest that it is characterized by what's happened in the two days of this Conference and the two days in November. Thank you very much.

Appendix A

Conference Program

Monday, March 4, 1974

8:15 a.m. **CONFERENCE REGISTRATION**

9:30 **CONFERENCE INTRODUCTION**
Welcome
Dr. Richard W. Roberts, *Director*
National Bureau of Standards
Opening Address
Honorable Betsy Ancker-Johnson
Assistant Secretary for Science and Technology
Department of Commerce

9:50 **CURRENT LEGISLATIVE PROPOSALS**
Arthur R. Miller, *Session Chairman*
Professor of Law, Harvard Law School
Honorable Edward I. Koch
Member of Congress, 18th District, New York
Honorable Barry M. Goldwater, Jr.
Member of Congress, 27th District, California

11:00 **COFFEE BREAK**

11:30 **CURRENT LEGISLATIVE PROPOSALS (cont'd)**
Jane L. Hardaway
Member, HEW Advisory Committee on Automated Personal Data Systems
Honorable Stanley J. Aronoff
Ohio State Senator
Honorable Mike Cullen
California Assemblyman

1:30 **LUNCH**

2:00 Peter F. McCloskey
President, Computer and Business Equipment Manufacturers Association

2:30 Robert W. Rector
Executive Director, American Federation of Information Processing Societies

2:45 **BREAK**

3:00 **COMPUTER SYSTEM ARCHITECTURE AND ACCESS CONTROLS**
Oliver R. Smoot, *Session Chairman*
Director, Industry Programs, Computer and Business Equipment Manufacturers Association
Security Architecture Using Encryption
Richard R. Keys
Honeywell Corporation
Phoenix, Arizona
Access Controls in Burroughs Large Systems
Harvey W. Bingham
Burroughs Corporation
Paoli, Pennsylvania
Systems Architecture for Security and Projection
James P. Anderson
James P. Anderson Company
Ft. Washington, Pennsylvania
Pragmatic Aproaches to Software Security
Richard L. Caplan
Advanced Computer Techniques Corporation
New York, New York

5:15 **ADJOURN**

Tuesday, March 5, 1974

8:15 a.m. **CONFERENCE REGISTRATION**

9:00 August G. W. Biddle
Executive Director, Computer Industry Association

Donn W. Sanford
Executive Director, Data Processing Management Association

9:45 John Christiansen
Chairman, Standards Committee, Association of Data Processing Service Organizations

10:15 **COFFEE BREAK**
A Systematic Approach to Data Security
R. L. Thomas
Robert H. Courtney
IBM Corporation
Armonk, New York

11:45 **Achieving Security in Computer Networks**
Peter S. Browne
General Electric Information Services Business Division

12:15 p.m. **OPEN FORUM**

1:00 **LUNCH**

2:00 **INFORMATION AND SECURITY MANAGEMENT**
Joseph F. Cunningham, *Session Chairman*
Executive Director, Association for Computing Machinery
Risk Analysis in Planning for Physical Security
Robert V. Jacobson
Sentor Security Group, Inc.
New York, New York
Security Considerations in Information System Design
Steven B. Lipner
MITRE Corporation
Bedford, Massachusetts
Auditing Current Systems
Donn B. Parker
Stanford Research Institute
Menlo Park, California

3:45 p.m. **CLOSING REMARKS**
Dr. Ruth M. Davis
Director, Institute for Computer Sciences and Technology
National Bureau of Standards

Appendix B

Executive Summary, Conference on Privacy and Security in Computer Systems

November 19–20, 1973

A two-day conference on Privacy and Security in Computer Systems was sponsored by and held at the National Bureau of Standards on November 19–20, 1973. Five hundred and ten people from government, the computer industry, and various public interest groups met to hear presentations of the needs and problems that confront governmental agencies in safeguarding individual privacy and protecting confidential data from loss or misuse.

Lawmakers at Federal, State and local levels of government are increasingly aware of the public's concern over computer-based recordkeeping and its implications for personal privacy. This concern has arisen partly out of fear of the impersonal super-efficient image that computers present and partly out of a reasoned concern over the expansion of governmental recordkeeping activities which computers make possible. Lawmakers are responding to this concern by proposing and enacting laws that are intended to specifically safeguard the rights and interests of individuals by prescribing the circumstances and the manner in which personal data can be collected, used and disseminated.

These legislative actions, if taken unilaterally, present the prospect of potentially conflicting requirements being imposed upon those charged with their implementation. Further, the technological capability needed to assure compliance with these requirements is not generally available. Compounding these problems areare increased public pressures to operate governments economically. These pressures foreclose the simplistic solution of using dedicated computers to process confidential data. yet the computer systems present available for resource sharing provide few techniques for controlling access to confidential data. These interrelated considerations strongly suggest that all of the legislative, technological and managerial solutions that can be brought to bear upon the problems of privacy and security must be effectively integrated so that a proper balance of needs and values in relation to costs can be achieved.

The assignment and acceptance of responsibilities for accomplishing this objective requires a recognition of the separable but interrelated components of the privacy and computer security problems. These may be identified as:

- *Protection of the privacy of the individual:* a responsibility of the legislative and judiciary branches of government.
- *Providing guidelines to assure information management is in compliance with legislative and judicial requirements for privacy:* a responsibility of government, management, and industry.
- *Development and application of the needed automation and information management technologies and products:* a responsibility of industry and the government.
- *Assessment and assignment of the costs of Security in Automation:* a responsibility of the government, industry and the public.
- *Management of information in automated recordkeeping systems:* a responsibility of management and information management technologists.

While the solutions for safeguarding privacy are to be found in legislative or regulatory sources, solutions for protecting confidential data are found in physical security measures and in the technological safeguards and procedures which permit controlled accessibility to the systems and data.

The broad scope of controlled accessibility precludes simple solutions. It embraces the use of specialized hardware and software with built-in protective features, mechanisms for authorizing access to systems and data, techniques for uniquely identifying individuals who are authorized to gain access, cryptographic devices and encryption algorithms to protect data during transmission among systems, and auditing or monitoring techniques for measuring system events of security interest.

While various techniques for access control exist, there are few guidelines for the application of these techniques. Lacking such guidelines, system users apply protection controls that are either inadequate or excessively costly for the degree of protection they require. The importance of considering the cost of

applying security measures cannot be over-emphasized, since security is always a cost vs. effectiveness trade-off. A highly important extension of this managerial concern is the question of how much the public wil be willing to pay for the protection of individual privacy and how the incremental cost for security is to be allocated among government, industry and the public.

Major needs for alleviating the problems of privacy, data confidentiality and computer security were identified on an initial basis. A realistic approach for addressing these needs could consist of parallel and coordinated efforts directed toward:

- Achieving a national coherence among laws defining the privacy rights of individuals and the basic information practices to be followed in protecting these rights.
- Establishing uniform management and technical procedures for effectively applying security measures. Important needs are techniques for assessing risks, determining threats and threat sources, evaluating alternative security measures, auditing the effectiveness of existing measures and physical security.
- Innovative applications of existing technology to enhance security effectiveness. Specific needs which are susceptible to solution in this way include the retrofitting of existing systems to satisfy new security requirements and the use of encryption techniques in civilian applications for protecting data during transmission.
- Research and development of new mechanisms and techniques where significant needs cannot be met satisfactorily by existing technology. Among the needs requiring this type of effort are self-protected computer systems which have the internal ability to enforce the access controls necessary for the prescribed level of security. Other needs include techniques for positively and uniquely identifying individuals who have authorization for access to the system and data and the development of secure network models for evaluating alternative network designs.
- A study of the costs of data confidentiality and security to build an understanding useful in making public choices about degrees of privacy desired by individuals and for allocating costs among the public, industry and government.

It is hoped that the Conference will stimulate the computer industry and other interested parties to propose specific approaches and solutions to the needs and problems outlined and will promote new initiatives for protecting data confidentiality in computer-based records systems.

A second Conference is planned for March 4–5, 1974, which will provide an opportunity for the presentation of proposed technological and regulatory solutions to the computer security needs and problems identified in this Conference.

NBS-114A (REV. 7-73)

U.S. DEPT. OF COMM BIBLIOGRAPHIC DATA SHEET	1. PUBLICATION OR REPORT NO. NBS-SP-404	2. Gov't Accession No.	3. Recipient's Accession No.

4. TITLE AND SUBTITLE

Approaches To

PRIVACY and SECURITY in COMPUTER SYSTEMS

5. Publication Date: September 1974

6. Performing Organization Code

7. AUTHOR(S): Clark Renninger

8. Performing Organ. Report No.

9. PERFORMING ORGANIZATION NAME AND ADDRESS

NATIONAL BUREAU OF STANDARDS
DEPARTMENT OF COMMERCE
WASHINGTON, D.C. 20234

10. Project/Task/Work Unit No.

11. Contract/Grant No.

12. Sponsoring Organization Name and Complete Address (*Street, City, State, ZIP*)

13. Type of Report & Period Covered: Final

14. Sponsoring Agency Code

15. SUPPLEMENTARY NOTES

16. ABSTRACT (A 200-word or less factual summary of most significant information. If document includes a significant bibliography or literature survey, mention it here.)

This publication summarizes and contains the proceedings of a conference held at the National Bureau of Standards on March 4-5, 1974 to continue the dialog in search of ways to protect confidential information in computer system.

Proposals are presented for meeting governmental needs in safeguarding individual privacy and data confidentiality that were identified at a conference held in November 1973. Among the proposals are the enactment of privacy legislation, improved computer system architecture and access controls, information and security management guidelines and the development of a systematic, balanced approach to system security.

The proposals were presented by legislators, citizens, computer industry associations and companies, professional societies, and public interest groups.

17. KEY WORDS (*six to twelve entries; alphabetical order, capitalize only the first letter of the first key word unless a proper name, separated by semicolons*)

Computer systems; confidentiality; privacy; privacy and security; security.

18. AVAILABILITY

[X] Unlimited

[ ] For Official Distribution. Do Not Release to NTIS

[X] Order From Sup. of Doc., U.S. Government Printing Office Washington, D.C. 20402, SD Cat. No. C13, 10:404

[ ] Order From National Technical Information Service (NTIS) Springfield, Virginia 22151

19. SECURITY CLASS (THIS REPORT)	21. NO. OF PAGES
UNCLASSIFIED	84
20. SECURITY CLASS (THIS PAGE)	22. Price
UNCLASSIFIED	$1.20

USCOMM-DC 29042-P74

BEST COPY AVAILABLE

NBS TECHNICAL PUBLICATIONS

PERIODICALS

JOURNAL OF RESEARCH reports National Bureau of Standards research and development in physics, mathematics, and chemistry. Comprehensive scientific papers give complete details of the work, including laboratory data, experimental procedures, and theoretical and mathematical analyses. Illustrated with photographs, drawings, and charts. Includes listings of other NBS papers as issued.

Published in two sections, available separately:

- **Physics and Chemistry (Section A)**

Papers of interest primarily to scientists working in these fields. This section covers a broad range of physical and chemical research, with major emphasis on standards of physical measurement, fundamental constants, and properties of matter. Issued six times a year. Annual subscription: Domestic, $17.00; Foreign, $21.25.

- **Mathematical Sciences (Section B)**

Studies and compilations designed mainly for the mathematician and theoretical physicist. Topics in mathematical statistics, theory of experiment design, numerical analysis, theoretical physics and chemistry, logical design and programming of computers and computer systems. Short numerical tables. Issued quarterly. Annual subscription: Domestic, $9.00; Foreign, $11.25.

DIMENSIONS/NBS (formerly Technical News Bulletin)—This monthly magazine is published to inform scientists, engineers, businessmen, industry, teachers, students, and consumers of the latest advances in science and technology, with primary emphasis on the work at NBS.

DIMENSIONS/NBS highlights and reviews such issues as energy research, fire protection, building technology, metric conversion, pollution abatement, health and safety, and consumer product performance. In addition, **DIMENSIONS/NBS** reports the results of Bureau programs in measurement standards and techniques, properties of matter and materials, engineering standards and services, instrumentation, and automatic data processing.

Annual subscription: Domestic, $6.50; Foreign, $8.25.

NONPERIODICALS

Monographs—Major contributions to the technical literature on various subjects related to the Bureau's scientific and technical activities.

Handbooks—Recommended codes of engineering and industrial practice (including safety codes) developed in cooperation with interested industries, professional organizations, and regulatory bodies.

Special Publications—Include proceedings of high-level national and international conferences sponsored by NBS, precision measurement and calibration volumes, NBS annual reports, and other special publications appropriate to this grouping such as wall charts and bibliographies.

Applied Mathematics Series—Mathematical tables, manuals, and studies of special interest to physicists, engineers, chemists, biologists, mathematicians, computer programmers, and others engaged in scientific and technical work.

National Standard Reference Data Series—Provides quantitative data on the physical and chemical properties of materials, compiled from the world's literature and critically evaluated. Developed under a world-wide program coordinated by NBS. Program under authority of National Standard Data Act (Public Law 90-396). See also Section 1.2.3.

Building Science Series—Disseminates technical information developed at the Bureau on building materials, components, systems, and whole structures. The series presents research results, test methods, and performance criteria related to the structural and environmental functions and the durability and safety characteristics of building elements and systems.

Technical Notes—Studies or reports which are complete in themselves but restrictive in their treatment of a subject. Analogous to monographs but not so comprehensive in scope or definitive in treatment of the subject area. Often serve as a vehicle for final reports of work performed at NBS under the sponsorship of other government agencies.

Voluntary Product Standards—Developed under procedures published by the Department of Commerce in Part 10, Title 15, of the Code of Federal Regulations. The purpose of the standards is to establish nationally recognized requirements for products, and to provide all concerned interests with a basis for common understanding of the characteristics of the products. The National Bureau of Standards administers the Voluntary Product Standards program as a supplement to the activities of the private sector standardizing organizations.

Federal Information Processing Standards Publications (FIPS PUBS)—Publications in this series collectively constitute the Federal Information Processing Standards Register. The purpose of the Register is to serve as the official source of information in the Federal Government regarding standards issued by NBS pursuant to the Federal Property and Administrative Services Act of 1949 as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973) and Part 6 of Title 15 CFR (Code of Federal Regulations). FIPS PUBS will include approved Federal information processing standards information of general interest, and a complete index of relevant standards publications.

Consumer Information Series—Practical information, based on NBS research and experience, covering areas of interest to the consumer. Easily understandable language and illustrations provide useful background knowledge for shopping in today's technological marketplace.

NBS Interagency Reports—A special series of interim or final reports on work performed by NBS for outside sponsors (both government and non-government). In general, initial distribution is handled by the sponsor; public distribution is by the National Technical Information Service (Springfield, Va. 22151) in paper copy or microfiche form.

Order NBS publications (except Bibliographic Subscription Services) from: Superintendent of Documents, Government Printing Office, Washington, D.C. 20402.

BIBLIOGRAPHIC SUBSCRIPTION SERVICES

The following current-awareness and literature-survey bibliographies are issued periodically by the Bureau:

Cryogenic Data Center Current Awareness Service (Publications and Reports of Interest in Cryogenics). A literature survey issued weekly. Annual subscription: Domestic, $20.00; foreign, $25.00.

Liquefied Natural Gas. A literature survey issued quarterly. Annual subscription: $20.00.

Superconducting Devices and Materials. A literature survey issued quarterly. Annual subscription: $20.00. Send subscription orders and remittances for the preceding bibliographic services to the U.S. Department of Commerce, National Technical Information Service, Springfield, Va. 22151.

Electromagnetic Metrology Current Awareness Service (Abstracts of Selected Articles on Measurement Techniques and Standards of Electromagnetic Quantities from D-C to Millimeter-Wave Frequencies). Issued monthly. Annual subscription: $100.00 (Special rates for multi-subscriptions). Send subscription order and remittance to the Electromagnetic Metrology Information Center, Electromagnetics Division, National Bureau of Standards, Boulder, Colo. 80302.